Guidance for Schools

Safe Use of Images

City and County of Swansea

Education Department

Initial release.	JM	01/12/2009
Second release.	EOR	25/04/2018

Safe Use of Images

Introduction

This guidance is aimed at helping you understand how to best make use of children's photographs ("images") as well as images you may find via other sources. It may also help you to understand some of your responsibilities in regards to privacy and the secure storage of data and information.

This guidance does not remove your responsibilities in relation to safeguarding, data protection, or the privacy of individuals.

It is written in Plain English to ensure clarity.

You can seek further advice on rights and responsibilities from expertise within the Education department, ICT Services, and Welsh Government, as well as other organisations.

You should especially seek guidance and up to date information from the Information Commissioner's Office ("ICO").

- https://ico.org.uk/for-organisations/education/

The intended audience for this guidance is:

- Local Authority Staff (within the Education department),
- Staff at Pupil Referral Units and those working with Looked After Children,
- School non-teaching staff within Swansea,
- School teaching staff within Swansea.

What this guidance is:

- A brief introduction to data security within schools;
- A summary of how to best make use of children's photographs ("images");
- A summary of how to best make use of other images; and
- A brief overview of your responsibilities in relation to data protection.

What this guidance is not:

- A complete guide to data security, GDPR, or your statutory responsibilities;
- A policy on data security requirements;
- A replacement for statutory requirements, legislation, or legal advice; or
- An absolution of your individual responsibilities.

Safe Use of Images

Introduction

Communication with parents, the local community, and other organisations is an important element of both managing and marketing a school in the modern era. However, balanced with this is the responsibilities of ensuring data protection and individual privacy, as well as preventing the infringement of copyright.

It is paramount that schools prioritise their responsibility to protect the rights of the individual pupil or parent, visitor, governor, or member of staff.

This guidance is designed to assist schools in establishing a sensible policy that covers the appropriate use of images of pupils and parents, visitors, governors, and members of staff. It also offers advice in regards to preventing the infringement of copyright.

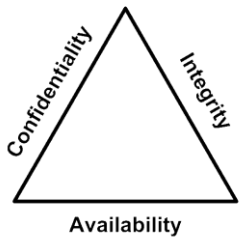
For full guidance and legal information, schools should seek advice from the Information Commissioner's Office ("ICO"), and Department for Education ("DfE").

- https://www.ico.gov.uk/
- https://ico.org.uk/for-organisations/education/
- https://www.gov.uk/government/publications/data-protection-toolkit-for-schools

C.I.A.

When thinking about the protection of information, you should consider the three principles of Confidentiality, Integrity, and Availability:

1. Confidentiality – Ensure information remains private.
2. Integrity – Ensure information remains accurate.
3. Availability – Ensure information is available.



The C.I.A. triad is covered in more detail through a wide array of training materials and resources including the following training materials available to Swansea Local Authority staff members on *LearningPool*:

1. Data Protection and Security
2. Cyber Security
3. Safeguarding and Protection of Children

- https://swansea.learningpool.com/

Safe Use of Images

Data Security and Types of Photographs

Government Security Classification

The Government of the United Kingdom operates a simple to understand Government Security Classification Policy. The policy defines three categories of data security.

OFFICIAL	SECRET	TOP SECRET
The majority of information that is created and processed within the public sector.	Very sensitive information that justifies heightened protective measures to defend against determined and capable threat actors.	The most sensitive information requiring the highest levels of protection from the most serious threats.

In the Information Security Guidance for Schools publication, Welsh Government have defined information processed within the school environment to be in the OFFICIAL category.

- http://gov.wales/docs/dcells/publications/160817-security-guidance-en.pdf *(Data Classification, Page 5)*

According to the Information Security Guidance for Schools document issued by Welsh Government, in relation to OFFICIAL data you should:

- Protect against deliberate compromise by automated or opportunistic attacks;
- Aim to detect actual or attempted compromise and respond.

Types of Photographs (“Images”)

Broadly, photographs (“images”) taken or used in the school environment may be described as one of the following:

1. Photographs (“images”) of individuals, or groups of people.
2. Photographs (“images”) obtained for evidencing individual or group work.
3. Photographs (“images”) obtained for the purpose of teaching.

Copyright not-withstanding; for each use case, the capture, storage, and use of photographs requires a legal basis.

Safe Use of Images

Seeking Consent

General Data Protection Regulation ("GDPR") as enacted in the United Kingdom defines different age categories in regards to **gaining consent**. It also clearly defines that consent must be given freely, not coerced. Individuals (or those acting on their behalf), have the right to withdraw consent at any time.

School Type	Age Group	Consent
Primary	3-11	Parents
Secondary	11-13	Parents
Secondary	13-16	Pupils
Sixth Form	16+	Pupils

For children under the age of 13, schools need to seek consent from whoever holds parental responsibility for the child. Children retain the same rights as their parents in relation to rectification, objection to processing, and erasure.

- https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/applications/children/

Parental consent expires when the child reaches the age at which they can consent for themselves; therefore, schools need to review and refresh consent.

Consent requests should be concise, separate from other terms and conditions, and easy to understand. Consent requests should include:

- School/organisation name;
- Names of any third party data controllers who will rely on the consent;
- Why you want the photographs;
- What you will do with the photographs; and
- How individuals can withdraw consent.

Schools must actively ask people to opt-in, schools cannot assume that they will opt-out. Each use case for photographs should be separate, to allow granular consent.

Schools should keep records of consent – who consented, when, how, and what they were told at the time consent was given.

If any of the purposes for the photographs change after consent is obtained, the consent will need to be refreshed.

- https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/

Safe Use of Images

Public Display and Consent

The General Data Protection Regulation ("GDPR") is an evolution of the Data Protection Act. The GDPR brings new rights, rules, and guidance as well as a strengthened enforcement policy.

GDPR requires schools to provide clarity and accountability in relation to the use of images in a school environment.

It does not require consent for each individual photograph ("image"), but **it does require explicit opt-in consent for each type of usage** you may wish to undertake.

Accountability relates to providing the individual with information on who may take the photographs, how they may be stored and for how long, what will happen in the event of a data breach, who to make a complaint to, what rights the individual has, and how to enact the individuals rights.

For children under the age of 13 in the United Kingdom, an individual with parental responsibility for the child may make decisions on behalf of the child.

- https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/

For example;

If you currently have consent to share photographs of children on *"social media"*, this is not clear; *"social media"* is broad and can suggest a diverse range of applications and websites; **you will need to clarify the usage**.

If you currently have consent to share photographs of children on *"Twitter"* and then decide to share their photographs on *"Facebook"*, then you may be in breach of GDPR, as you did not obtain consent for sharing on *"Facebook"*.

If you currently have consent to use photographs of children on *"Twitter"* **and** *"Facebook"* and do not use photographs in any other location, then you are not in breach providing you do not use them in another location.

The above examples are not exhaustive and include social media websites; GDPR does not only cover social media.

Schools need individual consent for all methods and locations that you store and share photographs ("images").

Safe Use of Images

Evidencing Work – Other Lawful Basis

It may be required for a school to keep physical copies, photographs and/or digital scans of work undertaken by a pupil in order to evidence their educational progress, academic achievements, and work undertaken during schooling.

This evidence may be required;

a) For the day to day management and operating of a school;
b) To provide evidence of work to local and national government;
c) To provide evidence of work to support services (e.g. EMAU);
d) To provide evidence of work to inspectors (e.g. Estyn); and
e) To provide evidence of work to examination organisations.

- https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/

Data, including photographs and images (including both digital and/or physical) that are for the purpose of *Evidencing Work*, that are not shared publicly or used for any purpose other than evidencing work, may not require consent.

In these situations, there is likely to be another legal basis for taking and storing the photographs and/or images, as defined in Article 6 of the GDPR, as well as the conditions for processing *"special categories of data"* as outlined in Article 9.

Photographs and images evidencing work for these purpose might be processed as a necessity for **compliance with a legal obligation *(Article 6, 1c)*. They may also fall in to the area of legitimate interests *(Article 6, 1f)*.**

Photographs and images evidencing work for the purpose of submitting to examination organisations may be considered as **necessary for the performance of a contract or to take steps prior to entering into a contract *(Article 6, 1b)*, or legitimate interests *(Article 6, 1f)*.**

Photographs related to providing education (i.e. evidencing work) may fall under the public task purposes, but after the child has left the school this argument becomes weak and may not be lawful; permission to retain beyond their time in school (if required) should be sought. For example, if the child is in a display showing a scientific experiment being done that you wish to retain as a learning resource for future years.

Schools should seek advice on which definition suits the photographs or images that they are seeking to make use of. Remember; each use case and the accountability for it must be clearly explained to pupils and those with parental responsibility.

Safe Use of Images

CCTV (Security Cameras)

Schools need to ensure that they have undertaken Data Protection Impact Assessments ("DPIA") to document the potential impact on individuals' privacy. Schools should also regularly review whether CCTV is still the best security solution.

If your security cameras are likely to overlook any areas which people may regard as private (e.g. a neighbouring house), you should consider where to install them and if at all possible restrict the view to minimise intrusion.

Fixed camera technologies may be more appropriate than Pan-Tilt-Zoom cameras. Camera systems that records sound will be significantly more intrusive and require more justification than one without that capability.

For internal school security cameras, schools should consider that **there may be a greater expectation of privacy in certain areas, such as locker rooms and changing areas.**

Schools should have a CCTV Policy that covers the use of CCTV, and they should have a nominated individual who is responsible for the operation of the CCTV system.

The CCTV Policy should cover the purposes the school are using CCTV for and how they will handle this information, including guidance on disclosures and recording. It is good practice to assign day-to-day responsibility for CCTV to an appropriate individual.

The individual should ensure that the school sets standards, has procedures and that the system complies with legal obligations including individuals' rights of access.

The CCTV Policy should establish a process to recognise and respond to individuals or organisations making requests for copies of the images on your CCTV footage and to seek prompt advice from the Information Commissioner's Office where there is uncertainty.

Further advice and support on the use of CCTV and responsibilities can be found on the Information Commissioner's Office website:

- https://ico.org.uk/for-organisations/guide-to-data-protection/cctv/

Safe Use of Images

Marketing, Advertising, and Promotional Media

Schools may seek to use photographs ("images") of pupils for the purposes of marketing, advertising, and promoting the school. Traditionally it may not be thought of as marketing and advertising, and yet **using photographs on a school website or in a prospectus very much do exist under the concept of marketing.**

This kind of use of photographs would be need to be consent based.

Remember; a school needs to obtain separate consent for each of the different processing activities. For example; just because a parent has consented for their child's photograph to be used on the school website, does not justify use in a newsletter or prospectus. The school must obtain consent for all of the processing activities, in a clear manner that explains each use case.

Using photographs of pupils for marketing purposes should not be considered under the concepts of legitimate interests or legal obligation. Although it is in the legitimate interests of the school to promote itself, it may not be in the legitimate interests of the pupil to participate in that promotion.

For example;

A group of pupils are photographed during a STEM lesson and the photograph is used in the school prospectus only. **Parental consent was given in relation to all pupils involved and the photograph is not used for any other purpose.** As consent was sought prior to the photograph being taken, this is acceptable.

The same photograph is then posted on to Twitter and the school website, but consent was not clearly requested for these two separate use cases. **This is unacceptable and in breach of GDPR.**

- https://ico.org.uk/for-organisations/education/

When taking photographs for marketing material, including social media; always remember to be conscious of appropriateness, inclusiveness, and respectability.

- Always ensure that pupils are appropriately clothed;
- Do not take photographs that would humiliate or negatively impact;
- Promote diversity and inclusiveness;
- Always gain consent prior to taking photographs.

Safe Use of Images

Building Passes (Photo ID)

Photographs ("images") of pupils, members of staff, visitors, and governors taken for building passes are considered personal data. As these images are likely to be stored electronically and with other personal data, it is important to carry out a Data Protection Impact Assessment ("DPIA").

Photographs used for building passes (i.e. identity management), may be essential for performing the public task of the school, but should to be deleted once the pupil is no longer in that setting, as it is no longer needed for the purpose for which it was held.

Some schools may make use of biometric data; e.g. facial recognition or the use of fingerprinting. GOV.UK have provided specialist advice related to this topic:

- https://www.gov.uk/government/publications/protection-of-biometric-information-of-children-in-schools

Personal Use (e.g. Parents and Grandparents)

GDPR permits parents and grandparents to take photographs and videos of their children for *personal use*. **It is important to note the difference between personal and public use.** Parents and grandparents would not be permitted to publicly display (e.g. on social media) photographs and videos that contained other children.

For example;

A parent takes photographs of their child and some friends taking part in Sports Day to put in a family album. These are for personal use and it is an acceptable use case under GDPR.

A grandparent wishes to video a nativity play that their grandchildren are involved with, to re-watch with close family at home. These are for personal use and it is an acceptable use case under GDPR.

A parent takes photographs of their child and some friends taking part in Sports Day to share publicly on *Twitter and Facebook*. This is not personal use and is not acceptable.

It is not unreasonable for a school to ask parents to sign a memo of understanding that explains that resulting photographs or videos are for personal use only and must not be sold, shared online, or used for any other purpose.

Safe Use of Images

Existing Photographs (Prior to 25 May 2018)

Schools will have many photographs and images that date prior to GDPR legislation becoming enforced in the United Kingdom. **Schools will need to be able to prove that they have the correct legal basis (consent, legal obligation, etc.) to hold the photographs, images, and data.**

When using consent as a legal basis, each use case needs to have a specific opt-in, and without an opt-in, the photographs are not likely to be compliant with GDPR. It is not enough to have a parental signature agreeing to photographs being taken *"for social media"*, or *"for school promotion"*.

If a school cannot prove how parents and/or pupils opted in to a specific use case, then the school will need to ask them to opt-in again, ensuring clarity and accountability.

- https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/

External Photographers

Where-ever possible, external photographers should be DBS (formerly CRB) checked and from a reputable source. **Opt-in consent should be sought from pupils or those with parental responsibility if the pupils are aged under 13, prior to the photographers work being conducted.**

Ensure that you have the backing of your school's governing body prior to the use of any external photographers. There may be a reason why it is not appropriate.

The external photographer must, to all who must consent, explicitly make clear all purposes for which they will use the photographs they will be taking.

Many schools welcome the local press in to school to report on special events and successes. This can be an important vehicle for raising the profile of the school in the local community and celebrating achievement school and individual achievement.

Be wary of allowing names to be printed and fully ensure that all involved have consented in advance.

Only allow interviews if opt-in consent has been obtained in advance and that the pupil and those with parental responsibility are aware in advance of the reason for and content of the interview.

Safe Use of Images

Copyright

Copyright is the right given to authors and creators of works to control the exploitation of their works. The right broadly covers copying, adapting, issuing copies to the public, performing in public and broadcasting the material.

Copyright arises automatically and does not depend on the completion of any formalities, such as registration.

Photographs and images, including icons, logos, and graphics, obtained from the internet are also subject to copyright laws.

The first owner of copyright is usually the author or artist of the work. The major exception is **where such work is made in the course of employment, in which case the employer owns the copyright.**

Commissioning and paying for work does not procure the copyright, unless the commissioning contract agrees otherwise.

The United Kingdom government provide advice and guidance on copyright:

- https://www.gov.uk/copyright

Copyright lasts for a minimum of the life of the author or creator plus 50 years, and at least 25 years for photographs. The length of the copyright depends on the type of work and how long ago the work was created.

The following summary table is provided by the GOV.UK:

Type of Work	Copyright Usually Lasts
Written, dramatic, musical and artistic work.	70 years after the author's death.
Sound and music recording.	70 years from when it's first published.
Films.	70 years after the death of the director, screenplay author, and composer.
Broadcasts.	50 years from when it's first broadcast.
Layout of published editions of written, dramatic, or musical works.	25 years from when it's first published.

Safe Use of Images

Obtaining Images from the Internet

All photographs and images on the internet have an owner. It is the responsibility of the school and the individual at the school to ensure they are not in breach of copyright law, by ensuring that any photographs or images used are:

- Either in the public domain (i.e. no longer under copyright);
- Licensed for free use (e.g. Crown Copyright, Creative Commons, etc.);
- Paid and licensed for use (e.g. purchased from a photographer); or
- Owned by the school and licensed for use.

In the past, schools may have saved images from Google Images or other similar search engines, and made use of these images in presentations and/or on their website. This practice is not lawful and is best avoided unless the individual can be absolutely certain that the copyright holder of the image permits this usage.

There are many websites where you can obtain royalty free, free to use, photographs and images. There are also many websites where you can obtain paid and licensed high quality photographs and images. The following are examples of both (not endorsements).

Royalty Free, Free to Use:

- https://www.pexels.com/public-domain-images/
- http://www.ibiblio.org/wm/paint/
- https://openclipart.org/

Paid and Licensed, High Quality:

- https://photodune.net
- https://graphicriver.net
- https://www.istockphoto.com/gb

Safe Use of Images

Staff Use of Personal Devices

To avoid any misunderstandings, mistrust, and potential loss of data, **staff at schools should not store photographs ("images") related to work (i.e. of pupils, parents, visitors, or governors), on their personal devices – including mobile phones.**

If the personal mobile phone or laptop was stolen and contained pupil photographs from the school, this would still need to be reported to the Information Commissioner's Office and may raise serious questions about the storage and security of data.

Similarly, if allegations of misconduct were made, it would be much more difficult to refute than if there were no pupil photographs stored on personal devices.

- https://ico.org.uk/for-organisations/report-a-breach/

If the personal mobile phone or laptop was stolen and did not contain pupil photographs, or other school related work, then this would not need to be reported to the Information Commissioner's Office ("ICO").

If members of staff are friends or relatives engaging in shared activities outside of the work place, then photographs related to them, but not to their work, taken on a mobile device may be considered for personal use only, and therefore not subject to the same restrictions.

However, equal care should be undertaken to ensure that these photographs are not stored on work-related devices (e.g. a school-owned laptop or phone).

On school trips to locations outside of the school environment, photographs can still be taken, providing all rules and regulations are followed. Members of staff should make use of photographic devices belonging to the school (e.g. phone, tablet, or camera), rather than their personal devices.

Although some may argue that it would be too costly to provide all members of staff with mobile phones, there are alternative options, including low cost tablet devices. Also, consider the financial and reputational cost of a fine from the Information Commissioner's Office ("ICO"), versus the purchase of a few devices.

The convenience of using a personal mobile phone should not be an excuse for ignoring the General Data Protection Regulation, or other data protection laws.

It should also be noted that locations outside of the school environment may impose their own additional requirements or prohibitions on the use of photography, and this should be identified, if possible, ahead of schedule.

Safe Use of Images

Best Practice

- Communicate the data privacy rights and responsibilities of your pupils, parents, visitors, governors, and members of staff.

- Communicate with pupils, parents, visitors, governors, and members of staff to request specific, clearly understood, opt-in consent where required.

- Ensure that you have undertaken relevant data protection impact assessments, created data security policies, and put in place procedures in place for handling and reporting data breaches.

- Always ensure you are using the most secure method you have available for storing and protecting personal data. Seek advice if you are unsure.

- Always ensure you have a justifiable reason to take photographs of pupils, parents, visitors, governors, and members of staff; *"it would be nice"* is not a good reason.

- Ensure you only share photographs publicly where you have appropriate opt-in consent to do so. Do not share without prior opt-in consent.

- Always ensure that all people you photograph are dressed appropriately and not in a manner that would cause concern or cultural upset.

- Never take or use photographs for any subject that may cause offense, embarrassment, upset, racism, or bullying. Instead, promote inclusiveness and diversity, respect, and compassion.

- Always respect a person's right to refuse to opt-in to photography appearing on social media, websites, or to be used for marketing purposes.

- Consider as a school, why a person may refuse a particular opt-in consent. Ask yourselves – does this person raise a good point? Should we be using and promoting that website to our pupils?

- Always consult with the case worker involved if you have a *Looked After Child*, prior to undertaking any photography, even if you have opt-in consent.

- If you are using CCTV; make sure that you have signs in visible locations that clearly state you are using CCTV and that it is recorded.

Safe Use of Images

Social Media – Safeguarding Children

Grooming and Kidnapping

There are many reports in the media related to the exploitation and kidnap of children who have had their personal details shared via social media websites. Predators may make use of information that a school posts publicly via social media in order to groom or kidnap a child.

As a school, you can reduce this risk by preventing staff from over-sharing and seeking consent prior to uploading photographs to a social media website.

Never share the names of pupil, parent or visitors via Twitter or other social media. Do not include initials (e.g. JD instead of Jane Davies), and do not include ages or dates of birth; even writing *"Happy birthday AA!"* on social media can be too much information**.**

A parent can recognise their child without needing personal information displayed.

Be sure that any certificate a pupil is holding whilst posing for a photograph, that you intend to share publicly, does not contain the pupil's name or other personal details.

You might for example wish to have a blank certificate as well as the real, and take the photograph whilst they hold the blank certificate. You can then re-use the blank certificate in the future.

Bullying and Racism

There is a misguided perception that anonymity exists on the internet by default. Sadly, because of this misguided perception, many people will use the internet (social media, chat applications, etc.) to bully and to promote racism.

As a school, you should be doing everything you can to discourage bullying and to promote the safeguarding of those who feel vulnerable. Furthermore, you should be encouraging an inclusive environment that welcomes diversity.

1. Consider how as a school you can include online activities as part of your anti-bullying and anti-racism policies; and how you can involve pupils.

2. Actively promote inclusiveness and rights respecting policies via your communication channels; whether those are online or offline based.

Safe Use of Images

Data Protection Impact Assessment

Data Protection Impact Assessments can help schools to identify and minimise the data protection risks related to projects and activities they may undertake.

Schools must do Data Protection Impact Assessments for certain types of data processing, as well as any other data processing that is likely to result in a high risk to individuals' interests.

The Information Commissioner's Office provides excellent guidance on how to undertake a Data Protection Impact Assessment.

- https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/

Reporting a Data Breach

Schools must report certain types of personal data breaches to the Information Commissioner's Office ("ICO") within 72 hours of becoming aware of the breach.

If the breach is likely to affect individuals (e.g. photographs leaked publicly where no consent was given), the school must also inform those individuals without undue delay.

Personal data breaches can include:

- Access by an unauthorised third party;
- Deliberate or accidental action (or inaction) by a controller or processor;
- Sending personal data to an incorrect recipient;
- Computing devices containing personal data being lost or stolen;
- Alteration of personal data without permission; and
- Loss of availability of personal data.

Detailed guidance is provided by the Information Commissioner's Office ("ICO").

- https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/

Schools should report personal data breaches via the Information Commissioner's Office ("ICO") website.

- https://ico.org.uk/for-organisations/report-a-breach/

Safe Use of Images

Key Terminology

The following abbreviations may be used in this guidance and due to increased awareness and use, are becoming increasingly common-place in the education sector.

DPA	**Data Protection Act 1998** http://www.legislation.gov.uk/ukpga/1998/29/contents
GDPR	**General Data Protection Regulation** https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/
ICO	**Information Commissioner's Office** https://ico.org.uk/
DfE	**Department for Education** https://www.gov.uk/government/organisations/department-for-education
C.I.A.	**Confidentiality, Integrity, Availability** https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/security/
CCTV	**Closed Circuit Television** https://ico.org.uk/for-organisations/guide-to-data-protection/cctv/
DPIA	**Data Protection Impact Assessment** https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/
DPO	**Data Protection Officer** https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-officers/

You may also find the key definitions described by ICO to be useful.

- https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/

The Department for Education has provided an invaluable guide entitled **Data Protection: Toolkit for Schools** *(DFE-00119-2018)*.

- https://www.gov.uk/government/publications/data-protection-toolkit-for-schools

Safe Use of Images

Example Photography and Video Policy

Photography and Video Policy

School Name

Created #DATE
Reviewed #DATES

PURPOSE

At #SCHOOL we use photographs and videos for a variety of purposes, including security, evidencing pupil work and attainment, newsletters, display boards, the school website, school prospectus, twitter, facebook, as well as other educational purposes.

We understand that parents may also wish to take photographs and videos of their children participating in school events for personal use.

We recognise both the benefits of photography and video in our school, as well as the risks involved. We recognise the rights individuals may possess in regards to privacy, data security, the right to rectification, and the right to erasure.

Under the legal obligations of the General Data Protection Regulation (GDPR), our school has specific responsibilities in relation to how photographs and videos are taken, stored, and retained.

Our school has implemented this policy on the safe use of photography and videos by staff and parents to reflect our protective ethos towards pupils' safety.

In order to ensure that, as far as possible, the use of photography and video is used safely at all times, this policy should be followed. This policy is applicable to all forms of visual media, including film, print, DVD, the internet, and broadcast.

LEGAL FRAMEWORK

This policy has due regard to legislation, including, but not limited to, the following:

- General Data Protection Regulation (GDPR) 2018; and
- Data Protection Act 1998.

This policy will be used in conjunction with, the following school policies:

- Data Protection;
- E Safety and Safeguarding;
- Acceptable Use of ICT.

This policy has been created with regard to the following guidance:

- Information Commissioner's Office (2018) – "Guide to the General Data Protection Regulation (GDPR)"
- Information Commissioner's Office (2017) – "Preparing for the General Data Protection Regulation (GDPR) - 12 Steps to Take Now"

DEFINITIONS

For the purposes of this policy:

"Personal use" of photography and videos is defined as the use of cameras and mobile phones to take photographs ("images") and recordings ("videos") of children by relatives, friends, or known individuals, e.g. a parent taking a group photo of their child and their friends at a school event.

These photographs and videos are only for personal use by the individual taking the photograph or video, and are not intended to be passed on to unknown sources, sold, or shared on the internet. The principles of GDPR do not apply to photographs and videos taken for this kind of personal use.

"Official school use" is defined as photography and videos which are used for school day-to-day "business" purposes, e.g. for building passes, and evidencing pupil work and attainment. These photographs and videos are likely to be stored electronically alongside other personal data. The principles of GDPR apply to photographs and videos taken for official school use.

"Media use" is defined as photography and videos which are intended for a wide audience, e.g. photographs of children taken for a local newspaper. The principles of GDPR apply to photographs and videos taken for media use.

Members of staff may also take photographs and videos of pupils for **"educational purposes"**. These are not intended for official school use, but may be used for a variety of reasons, such as school displays, special events, assessments, and celebrating positive achievements. The principles of GDPR apply to photographs and videos taken for educational purposes.

ROLES AND RESPONSIBILITIES

The Head teacher is responsible for:

- Submitting Consent Forms to parents at the beginning of the academic year, for pupils aged below 13; and submitting Consent Forms to pupils at the beginning of the academic year for pupils aged 13 and above.
- Ensuring that all photographs and videos are stored and disposed correctly; in line with the Data Protection Act 1998 and GDPR 2018.
- Deciding whether parents are permitted to take photographs and videos during school events.
- Communicating this policy to all governor and staff members, and the wider school community, such as parents.

The Designated Safeguarding Lead is responsible for:

- Liaising with case and social workers to gain consent for photography and videos of Looked After Children.
- Liaising with the Data Protection Officer, to ensure that there are no personal data protection breaches.
- Informing the Head teacher of any known changes to a pupil's security, e.g. child protection concerns, which would mean that participating in photography and video recordings could put them at significant risk.

The Data Protection Officer is responsible for:

- Informing and advising the school and its' members of staff about their obligations to comply with GDPR in relation to photographs and videos at school.
- Monitoring the schools compliance with GDPR in regards to the processing of photographs and videos.
- Advising the school on Data Protection Impact Assessments in relation to photographs and videos.
- Conducting internal audits, in regards to the school's procedures for obtaining, processing and using photographs and videos.
- Providing the required training to governors and members of staff, in relation to how GDPR impacts photographs and videos.

For pupils under 13 years of age, those designated with Parental Responsibility are responsible for:

- Completing the Photography and Video Consent Form on an annual basis.
- Informing the school in writing if there are any changes to their consent.
- Acting in accordance with this policy.

For pupils aged 13 years and older, they are responsible for:

- Completing the Photography and Video Consent Form on an annual basis.
- Informing the school in writing if there are any changes to their consent.
- Acting in accordance with this policy.

CONSENT

The Consent Form will be valid for the full academic year, including school term breaks, weekends, and public holidays, unless the person's circumstances change in anyway. E.g. if parents separate, or consent is withdrawn. Additional Consent Forms will be required if the person's circumstances change.

The school understands that consent must be a positive indication. It cannot be inferred from silence, non-response, inactivity, or pre-ticked boxes.

Consent will only be accepted where it is freely given, specific, informed, and an unambiguous indication of the individual's wishes.

Where consent is given, a record will be kept documenting how and when consent was given and last updated.

The school ensures that consent mechanisms meet the standards of GDPR. Where the standard of consent cannot be met, an alternative legal basis for processing the data will be found, or the processing will cease.

Staff members, governors, visitors, those with Parental Responsibility for pupils aged under 13 years, and Pupils aged 13 and above, will be asked to complete the Consent Form on an annual basis, which will determine whether or not they allow their child to participate in photographs and videos.

If there is a disagreement over consent, or if a person does not respond to a consent request, it will be treated as if consent has not been given, and photographs and videos will not be taken or published of the person who has not consented.

Everyone is entitled to withdraw or change their consent at any time during the academic year.

Those with Parental Responsibility for pupils under the age of 13, and Pupils aged 13 and above will be required to confirm on the Consent Form that they will notify the school if the pupil's circumstances change in any way, or if they wish to withdraw their consent.

For any Looked After Children ("LAC") pupils, the Designated Safeguarding Lead will liaise with the pupil's case worker, social worker, and carers or adoptive parents, to establish where consent should be sought.

Consideration will be given as to whether identification of a LAC pupil, or pupils that have been adopted, would risk their safety or security in any way.

Consideration will also be given to any pupils for whom child protection concerns have been raised. Should the Designated Safeguarding Lead believe that taking photographs and videos of any pupils would put their safety or security at further risk, greater care will be taken towards protecting their identity.

A list of all the names of pupils for whom consent was not given will be created by the Data Protection Officer and will be circulated to all members of staff. This list will be updated annually, when new consent forms are provided.

If any parent withdraws or changes their consent, or the Designated Safeguarding Lead reports any changes to a pupil's safety or security risk, or there are any other changes to consent, the list will also be updated and re-circulated.

GENERAL PROCEDURES

Photographs and videos of pupils will be carefully planned before any activity.

The Data Protection Officer will oversee the planning of any events where photographs and videos will be taken.

Where photographs and videos will involve Looked After Children, adopted pupils, or pupils for whom there are safety or security concerns, the Head teacher will liaise with the Designated Safeguarding Lead to determine a clear procedure.

When organising photographs and videos of pupils, the Head teacher, as well as any other members of staff involved, will consider the following:

- Can general shots of classrooms or group activities, rather than individuals, be used to fulfil the same purpose?
- Could the camera angle be amended in any way to avoid pupils being identified (e.g. from behind)?
- Will pupils be suitably dressed for the duration of the photography or the videoing? Are there any concerns related to clothing?
- Will pupils of different ethnic backgrounds and abilities be included within the photographs or videos, to support diversity?
- Would it be appropriate to edit the photographs or videos in any way? E.g. to remove logos or name badges which may identify pupils?
- Are the photographs and videos of the actual pupils completely necessary, or could an alternative method be used for the same purpose?

The list of all pupils of whom photographs and videos must not be taken will be checked prior to the activity. Only pupils for whom consent has been given will be able to participate, and those for whom consent has not been given will not be made to feel excluded or receive a lesser degree of education provision.

The members of staff involved, alongside the Head teacher and Data Protection Officer, will liaise with the Designated Safeguarding Lead if any Looked After Children, adopted pupils, or pupils for whom there are safety or security concerns is involved.

Only school equipment will be used to take photographs and videos of pupils; except for photographs and videos taken by parents and family members for personal use only. Members of staff will not use personal devices to take photographs or videos.

Members of staff will ensure that all pupils are suitably dressed before taking any photographs or videos, also taking in to account cultural sensitivities.

Where possible, members of staff will avoid identifying individual pupils. If names are required, only first names will be used, with prior consent.

The school will not use photographs or videos of any pupil who is subject to a court order.

The school will not use photographs of members of staff, governors, pupils, or parents, who have left the school, unless prior consent to do so has been obtained.

Photographs and videos that may cause any distress, upset, embarrassment, or cultural offense, will not be used or shared.

Any concerns relating to inappropriate or intrusive photography, or the inappropriate or intrusive publication of content, is to be reported to the Data Protection Officer.

ADDITIONAL SAFEGUARDING PROCEDURES

The school understands that certain circumstances may put a pupil's safety or security at greater risk and, thus, may mean extra precautions are required to protect their identity; especially when showing photographs and videos publicly.

The Designated Safeguarding Lead will, in known cases where a pupil is a Looked After Child or who has been adopted, liaise with the pupil's case and social worker, carers, and/or adoptive parents, to assess the needs and risks associated with the safety and security of the pupil.

Any measures required will be determined between the Designated Safeguarding Lead, case and social worker, carers, Data Protection Officer, and adoptive parents, with a view to minimise any impact on the pupil's day-to-day life. The measures implemented will be one of the following:

a) Photographs and videos can be taken as per usual school procedures;
b) Photographs and videos can be taken within school for educational purposes and official school use, but cannot be published in any online or external media.
c) Photographs and videos can be taken within school for educational purposes and official school use, and can be shared with local newspapers, but not published in any online or other external media.
d) No photographs or videos can be taken at any time, for any purpose.

Any outcomes will be communicated to all members of staff via a staff meeting, and the list outlining which pupils are not to be involved in any photographs or videos will be updated accordingly.

SCHOOL-OWNED DEVICES

Members of staff should only use school equipment to take photographs and record videos of pupils. This includes cameras, laptops, tablets, and mobile phones.

Where school-owned devices are used, photographs and videos will be provided to the school at the earliest opportunity, for secure storage, and removed from any other devices.

Members of staff will not use any personal device, including personal mobile phones, to take photographs or videos of pupils.

Photographs and videos taken by members of staff whilst on school visits externally, may be used for educational purposes where consent has been given. E.g. on in-school displays, or to illustrate the work of the school, or evidence the pupil's educational work.

Photographs and videos in digital form held in the school's secure storage area, are accessible to members of staff only. Photographs and videos are stored in labelled files, annotated with the date, and are only identifiable by year group / class number. No names are associated with photographs and videos.

The schools secure storage area is password protected and only members of staff have access to these passwords. These passwords are updated frequently to minimise the risk of access by unauthorised individuals.

USE OF PROFESSIONAL PHOTOGRAPHERS

If the school decides to use a professional photographer for official school photographs and school events, the Head teacher will:

- Obtain the support and guidance of the school governors;
- Ensure that any suitable DBS checks are verified;
- Provide a clear brief for the photographer about what is considered appropriate, in terms of both photography and behaviour;
- Issue the photographer with identification, which must be worn at all times;
- Inform parents and pupils in advance that a photographer will be in attendance at an event, and ensure that consent to both the taking and publication of photographs and videos has been obtained prior to the event.
- Not allow unsupervised access to pupils or one-to-one photograph sessions.
- Communicate to the photographer that any photographs or videos may only be used for the school's own purposes and that permission has not been given to use the photographs for any other purpose.
- Ensure that the photographer will comply with the requirements of GDPR.
- Ensure that if another individual, such as a parent or governor, is nominated to be a photographer, they are clear that the photographs and videos are not used for any other anything other than the purpose indicated by the school.

PERMISSIBLE PHOTOGRAPHY AND VIDEOS DURING SCHOOL EVENTS

If the Head teacher permits parents to take photographs or videos during a school event, parents will:

- Remain seated while taking photographs or videos during concerts, performances, and other events, unless standing is permitted by staff;
- Minimise the use of flash photography during performances;
- Ensure that the focus of any photographs or videos is their own children;
- Avoid disturbing others in the audience or distracting pupils when taking photographs or recording videos.

- Ensure that any photographs and videos taken at school events are exclusively for personal use and are not uploaded to the internet, shared on social media, or openly shared in other ways.
- Refrain from taking photographs and videos if and when requested to do so by staff. This may be temporarily or for the remainder of the event.

STORAGE AND RETENTION

Photographs and videos obtained by the school will not be kept for any longer than necessary. Paper documents will be shredded or pulped, and electronic files destroyed, once the data has reached a point where it should no longer be retained.

Any physical copies of photographs and videos held by the school will be annotated with the date on which they were taken and will be stored in a secure location. They will not be used other than for their original purpose, unless the Data Protection Officer has been consulted and consent is granted from the Head teacher and the subject person, or their parental representative if under 13 years of age.

The Data Protection Officer will review stored photographs and videos on a termly basis to ensure that all unwanted material has been deleted.

Parents of pupils under 13 years of age, and Pupils aged 13 and above, must inform the school in writing where they wish to withdraw or change their consent. If they do so, any related photographs and videos involving their children will be removed from the secure storage areas immediately.

When a person withdraws consent, it will not affect the use of any photographs or videos for which consent has already been obtained. Withdrawal of consent will only affect further processing.

Where a pupil's safety or security risk has changed, the Designated Safeguarding Lead will inform the Head teacher immediately. If required, any related photographs and videos involving the pupil will be removed from the school drive immediately. Any physical copies will be removed by returning to the person or by shredding, as may be appropriate.

Official school photographs and videos are held in secure storage areas, including the School Information Management System ("SIMS"), alongside other personal data, and are retained for the length of the pupil's attendance at the school, or longer, if necessary, e.g. due to a police investigation or other legal requirement.

Some educational records relating to former pupils of the school may be kept for an extended period for legal reasons, and also to enable the provision of references or academic transcripts.

This policy must be read in conjunction with all other school policies, including the school's CCTV Policy.

MONITORING AND REVIEW

This policy will be reviewed on an annual basis by the head teacher. The next scheduled review date for this policy is October 2018.

Any changes to this policy will be communicated to all governors and members of staff and, where appropriate, parents.

Safe Use of Images

Example Consent Form – Pupil's Under 13

Photography and Video Consent Form

School Name Academic Year #DATE - #DATE

Dear Parent,

During the course of the school year, we may sometimes wish to take photographs or video recordings of children within school or on school trips. Our school make use of photography and video a wide range of activities. These include:

- For evidencing pupil classwork and attainment; and
- Inclusion in our promotional material.

Some photographs taken and videos recorded may be necessary as part of our legal obligations, conditions of contract, and necessary to perform public tasks. These photographs will not be shared publicly and only used for their intended purpose. For example; to submit work to an examination organisation.

In addition, our school may invite an external photographer to the school each year to take official school photographs, and the school may also be visited by the media to take photographs for publication.

To comply with the Data Protection Act 1998 and General Data Protection Regulation 2018, and to protect your child's interests, we need to ask your consent, every school year, before the school or the media take photographs or video recordings of your child.

Please tick the relevant opt-in consent choices on the reverse of this Photography and Video Consent Form, sign, and return to the office no later than **#DATE**.

Parental Photography:
We understand that parents are very supportive of their children. Photographs taken and video recordings by parents and relatives of children at our school should be for personal use only; **"personal use"** photographs and videos must not be sold, shared online, or publicly in any other format.

There may arise occasions when our head teacher requests that photographs and videos are not taken. A copy of our Photography and Video Policy is available upon request. If you have any concerns, please contact our school office.

Please tick ✓ the relevant boxes where you give your consent to photographs and videos of your child being used for the described purpose. Please also remember to sign and date your Consent Form.

If you do not tick or we do not receive this consent form, we must assume you have not consented. Please also indicate whether you consent to your child's first name being associated with their image (we will not publicly share last names, ages, or dates of birth.)

	I consent to…	
	Use of Photos and Videos	**Sharing of First Name**
Internal items, e.g. displays around school.		
School Prospectus (Digital and Printed)		
School Newsletter (Digital and Printed)		
On School Website		
In Local Newspapers (e.g. Evening Post)		
On Television		
Via Webcam for Educational Purposes		
Radio Broadcasting		
YouTube		
Twitter		
Instagram		
Facebook		

I confirm that I have read and agreed to the terms contained within this Consent Form, and agree to inform the school, in writing, of any changes to my consent.

Signed: _____

Relationship to Child: _____

Date: _____

For Office Use Only:

Consent Form Received (Date): _____

Authorised (Name): _____

Authorised (Signature): _____

Audience

It is intended that this guide be read by educators in Swansea who seek advice in relation to the safe use of images related to schools.

Disclaimer

This guidance is written in good faith that the reader will take full responsibility for ensuring that they seek the proper legal advice, guidance, and fact checking prior to enacting anything contained within this guidance. The City and County of Swansea and the author of this guidance cannot take responsibility for the use or misuse of information described within this guidance.

It is recommended that all educators take time to learn about the importance of protecting and safeguarding children and vulnerable people, as well as the importance of safely handling personal data.

The information in this guidance is correct at time of writing. Digital platforms are subject to change and therefore as time progresses it is to be expected that the information in this guidance may become out of date. In such an event you should seek training and support from the Education department.

The existence of this guidance does not commit to future guidance being produced on the same platforms or technologies.

The information within this guidance is intended for educators in Swansea. Whilst it may have relevance to other areas of Wales, it is not intended as a replacement for any official documentation from the Information Commissioner’s Office or legal advice.