ELMGROVE PRIMARY SCHOOL AND NURSERY

Policy in relation to the use of images

November 2024

Next review November 2026

Introduction

Many school activities involve the taking and use of images. These may be undertaken as part of the curriculum, extra school activities, for publicity or to celebrate achievement.

At Elmgrove Primary School and Nursery we are aware of the potential for these aspects of teaching to be misused.

In order to safeguard our pupils and staff the following guidance is adhered to. The guidance applies to digital technology and resources used for storing and printing images.

Images taken at school events and concerts

Parents are made aware that images may be taken at these events when joining the school and are also asked to sign to agree that any images taken are intended for family/ private use only.

Images taken for personal use by parents/carers at school events in many cases do not fall into the Data Protection Act 2018 e.g. taking images at concerts and sports events. At such events the school needs to make parents aware that the images must be for private use only and that the selling or distribution without proper permission is illegal.

Those taken for official school use do, however, fall under the 2018 Data Protection Act and the subsequent GDPR guidance.

Parental Consent

Data Protection Act 2018 affects the official use of photography by educational settings as an image of a child is considered to be personal data. As recommended, we therefore seek consent from the parent before using images in school. This needs to be written consent. It is obtained by the parent as the child joins the school. No images are taken before this consent is received.

Even when we have permission, we check whether the child is also consenting to the images being taken before we take an image; if a child seems uncomfortable them we do not take the image.

Consent is generally sought for the whole period the child will be at the school.

Children in vulnerable circumstances e.g. victims of parental violence, those who are looked after should not have images taken without parental consent and/or social worker agreement.

Consent for adults
Schools also need consent from teachers and other adults who may appear in photographs/images. A consent form should be filled in. We seek separate consent to take parent's images if necessary. No images of parents or visitors should be taken or used without an individual consent form being completed.

Identification of the children and adults
Any image should not allow an unauthorised person to identify a child/adult or their whereabouts.

On photographs/images
If a first and surname are used – then no image should be used.
If an image is used – then no name is recommended, although first names can be used in some circumstances.

Staff should use **group images or class images** rather than close up images of individuals if possible.

See information below regarding the labelling of image files.

Existing Images
Existing or older images should only be used where consent was received. In addition, they should only be used online where consent has been given for publishing on line. If consent was never given, then it would be unwise to use the images. Please consult the Headteacher before using existing images. If an adult or child supplies a photograph to the school, then written consent should be given before using the photograph.
Images should be removed once their purpose has ended or within twelve months after a child leaves primary education or an adult leaves the school unless it has been agreed otherwise.

Types of images which are suitable
No images should ever be taken of children in what are commonly understood as non-public activities such as toileting or changing clothes, or which show body parts which are not usually visible in public settings. Children should be fully clothed. Images involving groups should be about the activity, not the individual child.

Capturing digital images and video
In order to avoid any allegations, images should be captured using a **school** mobile device (but not a phone unless authorised by the Headteacher).

Staff should **NEVER** use personal mobile technology to capture images and video.

Transfer of images
Images should be transferred as soon as possible using leads to the school media bank on the shared network.
Images on iPads are transferred as soon as possible after a lesson. They should then be deleted from the device. This is to ensure that the school retains control of how the pictures are used and minimises the risk of a breach of the Data Protection Act.

If we send images via email then this is not secure and there is a risk they may fall into the wrong hands. They should therefore be password protected before sending them or sent via egress switch secure email.

If we send images to a third party site for printing then we retain a copy of their privacy policy and ensure that we have signed agreement that both parties to adhere to safe practices around processing of the data. When content is uploaded to a third party website, it may be that the school no longer owns the images and they could be used by the website for other purposes such as promotions and publicity without the school consent. If we wanted to do this the parental consent form would need to be amended. The school should check whether this is possible in the first place as many sites are for personal use only.

A risk assessment should be completed for any sites or apps which are used to share, host or access images to identify possible dangers and what actions may need to be taken. Staff would need to be trained appropriately.

Storing digital images and video
Images should be stored in the media bank area on the shared network.

They should not be taken off site without permission from the Headteacher and should be encrypted and logged in and out. This would also apply to many 'apps' on smartphones and tablets.

Images should **NEVER** be stored on the desktop or iPad for longer than necessary, only on the server.
Images should **NEVER** be stored on a personal computer.
Ensure **image files are appropriately named** - do not have the child's name in the image file name or ALT tags if published on the web (see below for more information).

Deletion
Images are generally deleted once their purpose has ended or within twelve months after a child has completed their primary education or an adult leaves the school. Parents are made aware of this on the consent form.
Images are checked annually by the IT Technician and deleted if not needed in line with the policy.

To reduce the threat of inappropriate use we:

- Seek **parental permission** on entry to use images of pupils
- Never use the **first and last name** of a child on a picture, if we use the full name, then no image and if we use the image then no full name - this includes photographs taken for use in newspapers.
- Use **group images, class images** rather than close up images of individuals
- Ensure **image files are appropriately named** - do not have the child's name in the image file name or ALT tags if published on the web
- **Images are appropriately** stored on the school's network.
- Only use images of pupils in **suitable dress** to reduce the risk of inappropriate use
- Remove images as soon as they are finished with. We state clearly whether an image will be retained for further use and if so what use
- Creating a recognised procedure for checking websites, reporting the use of inappropriate images and responding to such a report.
- Consider the use of drawings and models instead of images.
- Do not manipulate images apart from removing badges to protect identity or 'cropping' images to fit.
- Advise staff that mobile phones and other personal mobile technology should be kept in the lockers/ locked away and can only be used in the staffroom and the offices and at breaktimes. Permission needs to be sought from the Headteacher if a member of staff needs to keep his/her mobile phone with them.

Further Technical advice
When saving pictures, ensure that the image file is appropriately named. Do not use pupils' names in image file names or in <ALT> tag references when published on the web. [An ALT tag is the HTML text describing a displayed image, used mostly for reasons of accessibility, since the tag can be voiced by screen readers]
Many schools are now using video as part of their Visual Literacy work. It is important that staff do not use software to 'rip-out' sections of copyrighted movies without permission.

Use of photos/video by children

This can be a useful tool to support learning. The use of equipment should be supervised carefully to ensure that images are appropriate. Children should be taught appropriate use of any equipment.

Parents should be made aware that children may be taking images of other children and should be informed whether these will be shared on line or whether they are for internal use only.

At Elmgrove children are not allowed to use their own equipment on site. Children are allowed to take a disposable camera on school journey but these are handed out during the day and collected in before the children go to their rooms in the evening. Please see the use of mobile technology policy.

School websites

The school website is an important, public-facing communication channel. Many prospective and existing parents find it convenient to look at the school's website for information and it can be an effective way to share the school's good practice and promote its work. We have put in place procedures and practice to ensure website safety. A senior member of staff oversees / authorises the website's content and checks suitability. It should be clear who has authority to upload content into sections of the website. In our case, this is the IT Technician or the Headteacher.

On the website we generally use group/paired photographs rather than photos of individual children. We do not use the name of individuals in a photograph. This reduces the risk of inappropriate, unsolicited attention from people outside the school. An easy rule to remember is:

• If the pupil is named, avoid using their photograph / video footage.
• If the photograph /video is used, avoid naming the pupil.

If we use video we take care to ensure that pupils aren't referred to by name on the video, and that pupils' full names aren't given in credits at the end of the film.

If showcasing examples of pupils work we use only first names, rather than their full names.

Parental permission is obtained before publishing any photographs, video footage etc. of pupils on the school website. Permission is obtained though the forms parents sign when a child joins the school.

If this is part of the actual website or in any other high profile public printed media additional permission is sought. This ensures that parents are aware of the way the image of their child is representing the school; a printed copy of the specific image should be attached to this form. A Parental Permission Form is an appropriate way of achieving this.

We try to use excerpts of pupils' work such as written work, scanned images of artwork or photographs of items designed and made in technology lessons. This

allows pupils to exhibit their work to a wider audience without increasing the risk of inappropriate use of images of pupils.
Links to any external websites should be thoroughly checked before inclusion on a school website to ensure that the content is appropriate both to the school and for the intended audience. Remember that the content of websites can change substantially, even in a short space of time. Staff should check all links regularly, not only to ensure that they are still active, but that the content remains suitable too.

Twitter
The same rules apply to uploading children's pictures on twitter as to uploading onto the school website. Parental permission is obtained before publishing any photographs, video footage etc. of pupils on the school Twitter page. Permission is obtained though the forms parents sign when a child joins the school.

Webcams
We only use webcams as part of our remote learning on Teams. We may use them within the school environment e.g. for assemblies. Teachers may use Teams to call a child at home if they are unable to attend school for a prolonged period of time. In this instance this will be scheduled with the parents. Students are not able to use Teams meetings unattended.

CCTV
School has CCTV. The separate policy alerts staff and parents to why it is there, what we use the images for and indicates who may wish to see the images. Areas with CCTV are signposted.

Professional Photographers
This includes the photographers who take individual and class photographs. The photographer is considered to be a data processor in relation to the data protection legislation and schools should seek assurances that they meet current standards in relation to data protection. We should ask them to confirm that they comply with the Data Protection Act 2018, the images will only be used for the specified purpose and will not be used in another context and they will not be disclosed to a third party without prior agreement. Evidence of DBS checks should be obtained and photographic ID should be seen on arrival.

Use of images by the media
Consent is sought from the parent.

Copyright
We are aware, as all schools should be that photographs obtained from the internet are subject to copyright and current procedures should be followed.

Education
Staff should report inappropriate use of images to the Headteacher and pupils should be taught who to report any inappropriate use of images to and understand the importance of safe practice. Staff and pupils also need to understand how to consider an external 'audience' when publishing or presenting work.

Appendix 1

DATA PROCESSING ADDENDUM

This Amendment Agreement is made on [XX Month Year]

BETWEEN

(1) [Add name and address] hereby referred to as the Controller.

(2) [Add name and address] hereby referred to as the Processor.

(hereinafter referred to as the "Parties")

BACKGROUND:

(A) The Controller processes Personal Data in connection with its business activities;

(B) The Processor processes Personal Data on behalf of other businesses or organisations;

(C) The Controller wishes to engage the services of the Processor to process Personal Data on its behalf.

IT IS AGREED AS FOLLOWS:

1. **Definitions and Interpretation.**

Agreement:	this Data Processing Agreement.
Business Day:	a day other than a Saturday, Sunday or public holiday in England when banks in London are open for business.
Data Protection Authority:	the relevant data protection authority is the Information Commissioners Office (ICO)

Data Protection Legislation:	means the Data Protection Act 2018 which incorporates the General Data Protection Regulation (GDPR), the Privacy and Electronic Communications (EC Directive) Regulations 2003 and any legislation implemented in connection with the General Data Protection Regulation which is the governing legislation that regulates data protection across the EEA. This includes any replacement legislation coming into effect from time to time.
Data Security Breach:	a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to the Shared Personal Data.
Parties:	means [Add names]

2.0 SCOPE

2.1 The purpose of this Data Processing Agreement is to describe the work to be carried out by the Processor in relation with the Agreement. This Data Processing Agreement forms an integral part of the Agreement hereof. This Data Processing Agreement shall be deemed to take effect from the effective date and shall continue in full force and effect until termination of the Agreement.

3.0 **DATA PROTECTION**

3.1 [Add Controller Name] is the data controller for the Personal Data and [Add Controller Name] is the Data Processor for the Personal Data. The Data Processor agrees to process the Personal Data only in accordance with Data Protection Legislation.

3.2 The Parties acknowledge that the Processor may process Personal Data on behalf of the Controller during the term of this Agreement. A description of the Personal Data and the processing activities undertaken by the Processor is set out in Appendix 1.

3.3 To the extent that the Processor processes Personal Data on behalf of the Controller in connection with this Agreement, the Processor shall:

3.3.1 Solely process the Personal Data for the purposes of fulfilling its obligations under this Agreement and in compliance with the Controller's written instructions as set out in this Agreement

and as may be specified from time to time in writing by the Controller;

3.3.2 Notify the Controller immediately if any instructions of the Controller relating to the processing of Personal Data are unlawful;

3.3.3 Ensure that its sub-contractors shall not transfer to or access any Personal Data from a Country outside of the European Economic Area without the prior written consent of the Controller;

3.3.4 Comply with the Controller's instructions in relation to transfers of Personal Data to a Country outside of the European Economic Area unless the Processor is required pursuant to applicable laws to transfer Personal Data outside the European Economic Area, in which case the Processor shall inform the Controller in writing of the relevant legal requirement before any such transfer occurs, unless the relevant law prohibits such notification on important grounds of public interest;

3.3.5 Ensure that any persons used by the Processor to process Personal Data are subject to legally binding obligations of confidentiality in relation to the Personal Data and shall ensure that only such persons used by it to provide the Services have undergone training in Data Protection and in the care and handling of Personal Data;

3.3.6 Not engage with any Sub-Contractor to carry out any processing of Personal Data without the prior written consent of the Controller, provided that notwithstanding any such consent the Processor shall remain liable for compliance with all of the requirements of this Contract including in relation to the processing of Personal Data;

3.3.7 Ensure that obligations equivalent to the obligations set out in this clause 2 are included in all contracts between the Processor and permitted sub-contractors who will be processing Personal Data;

3.3.8 Take appropriate technical and organisational measures against unauthorised or unlawful processing of Personal Data and

against accidental loss or destruction of or damage to Personal Data taking into account the harm that might result from such unauthorised or unlawful processing, loss, destruction or damage and the nature of the Personal Data to be protected including without limitation, all such measures that may be required to ensue compliance with Article 32 of the GDPR;

3.3.9 Taking into account the nature of the data processing activities undertaken by the Processor, provide all possible assistance and co-operation (including without limitation putting in place appropriate technical and organisational measures) to enable the Controller to fulfil its obligations to respond to requests from individuals exercising their rights under the Data Protection Legislation;

3.3.10 Maintain a record of its processing activities in accordance with Article 30(1) of the GDPR;

3.3.11 Assist the Controller in ensuring compliance with the obligations set out in Articles 32 to 36 of the GDPR taking into account the nature of the data processing undertaken by the Processor and the information available to the Processor, including (without limitation):

(a) Providing information and assistance upon request to enable the Controller to notify Data Security breaches to the Information Commissioner and / or to affected individuals and / or to any other regulators to whom the Controller is required to notify any data security breached; and
(b) Providing input into and carrying out data protection impact assessments in relation to the Processors data processing activities;

3.3.12 Upon termination of this Agreement, at the choice of the Controller, delete securely or return all Personal Data to the Controller and delete all existing copies of the Personal Data unless and to the extent that the Processor is required to retain copies of the Personal Data in accordance with applicable laws in which case the Processor shall notify the controller in writing of the applicable laws which require the Personal Data to be retained. In the event that the Personal Data is deleted or destroyed by the Processor, the Processor shall provide the

Controller with a certificate of destruction evidencing that the Personal Data has been destroyed or deleted;

3.3.13 make available to the Controller all information necessary to demonstrate compliance with the obligations set out in this clause 2 and allow for and contribute to audits, including inspections, conducted by or on behalf of the Controller or by the Information Commissioners Office (ICO) pursuant to Article 58(1) of the GDPR.

3.3.14 Indemnify the Controller from and against all costs, expenses (including legal and other professional fees and expenses), losses, damages, and other liabilities of whatever nature (whether contractual, tortious or otherwise) suffered or incurred by the Controller and arising out of or in connection with any breach by the Processor or any sub-contractors of this clause 2.

3.4 The Processor shall notify the Controller immediately by completing the Personal Data Breach Notification Form if:

3.4.1 the Processor or any sub-contractor engaged by on behalf of the processor suffers a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data; or

3.4.2 the Processor or any sub-contractor engaged by on behalf of the processor receives any data security breach notification, complaint, notice or communication which relates directly or indirectly to the processing of the Personal Data or to either party's compliance with the Data Protection Legislation.

And in each case the Processor shall provide full co-operation, information and assistance to the Controller in relation to any such data security breach, compliance notice or communication.

3.5 Upon request the Processor shall allow the Controller the ICO and its representatives access to the Processors premises, records and personnel for the purposes of assessing the Processors compliance with its obligations under this clause 2.

4.0 **TERMINATION**

4.1 The Controller may immediately terminate this Agreement on written notice to the Processor. The processor may not terminate this Agreement without the written consent of the Controller.

For and on behalf of [Add Company name]

……

For and on behalf of [Add Company name]

……

APPENDIX 1a
DATA PROCESSING ACTIVITIES

DESCRIPTION OF DATA

This Appendix 1a includes certain details of the processing of Personal Data as required by Article 28(3) GDPR.

Please outline the Personal Data which will be processed under this Agreement, including the Personal Data to which the Controller has defined as is relevant to the processing. For example please see below.

Name
Date of Birth
Telephone Number
Email address
IP address
Product details
Precise location data
[Add additional types of data]

CATEGORIES OF DATA SUBJECTS

The Controller has defined the following Data Subject categories from who the Personal Data as defined above will be collected.

Employees
Customers
Suppliers