

[REDACTED]

2 March 2020

Dear Mrs [REDACTED]

Case Reference Number [REDACTED]

I write to inform you that I have now completed my investigation into the inappropriate disclosure of the personal data of a child.

In summary, it is my understanding that a pupil at [REDACTED] (the 'School') was included in a class photo and the proof sent home to class parents although the parent had stated on consent forms that the child's photograph was not to be used outside school. The parent has advised us that this raises safeguarding issues.

Based on my assessment and the information you have provided, I have decided to issue [REDACTED], as controller for data processed by [REDACTED], with a reprimand in accordance with Article 58(2)(b) of the General Data Protection Regulation (the GDPR). The specific terms of the reprimand can be found towards the end of this letter.

Our consideration of this case

I have investigated whether [REDACTED] has complied with the following requirements of the GDPR:

- Article 5 (1) (a) which stipulates that personal data shall be "processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');

- Article 5 (1)(f) which stipulates that personal data shall be “processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical and organisational measures (‘integrity and confidentiality’)”;
- Article 5 (2) which states that “the controller shall be responsible for, and able to demonstrate compliance with, paragraph 1 (‘accountability’) and
- Article 33 which states that “the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.”

In response to our enquiries, [REDACTED] has provided the ICO with the following key information:

- the incident occurred despite the systems the School had in place. There were several contributing factors and it was not clear to a new member of staff that use ‘outside of school’ included class photographs. As a result of this incident, the School has compiled a ‘Vulnerable pupil list’ which is checked before any school activity where pupils may be photographed to ensure compliance with permissions. The School has reviewed and reworded the Home/School Agreement to make parents/carers aware that school photos are sent out to families with pupils in a particular class and to ensure that any ambiguity around wording has been eradicated;
- the School would have contacted the ICO immediately had it been advised to do so, or felt that any data breach had occurred. Additionally, the School did not report this to the ICO as it considered that there were no safeguarding risks to the child due to the swift action taken and that it considered that the parent was satisfied with the way the School had managed the risk and
- the incident was recorded under the child’s section of CPOMS (a safeguarding software package for schools).

Taking the above into account, we do not believe [REDACTED] has complied with the requirements outlined by the GDPR. More specifically, we consider [REDACTED] to have infringed Article 5 (2) for the following reasons:

- [REDACTED] failed to implement an appropriate procedure for the handling of pupils' images and
- [REDACTED] failed to consider reporting this incident to the ICO as a personal data breach - it does not consider that a breach has occurred.

We also consider [REDACTED] to have infringed Article 5 (1)(a) for the following reason:

- the processing of the pupil's image occurred in the absence of a lawful basis as required by Article 6.

In addition, we consider [REDACTED] to have infringed Article 5 (1)(f) for the following reason:

- the system in place at the time of the breach relied on the member of staff who was organising the class photo to understand that use of photos outside of school included class photographs.

Details of reprimand

The reprimand has been issued in respect of the following processing operations that have infringed the GDPR:

- processing of personal data in breach of the principles and guarantees set out in Article 5 (1)(f) and / or (a) and
- failing to implement organisational measures across the organisation in breach of the obligation set out in Article 5 (2), as the School cannot demonstrate accountability with the principles.

Further action required

Due to this, the Commissioner considers that [REDACTED] needs to take certain steps to improve compliance with the GDPR. We therefore strongly recommend your organisation implements the following measures:

- review and revise, where necessary, all policies and procedures in place in relation to the use of photographs to ensure that they are sufficiently robust.

These should include guidance on the practical application of procedures to prevent inappropriate disclosures;

- ensure school staff and governors receive appropriate training so that they are aware of and understand their obligations under the GDPR, with particular emphasis on security, personal data breaches and accountability and
- enforce all policies and procedures which are already in place and reiterate them to staff and governors on a regular basis, such as annually or as soon as changes are made. All staff and governors should also sign a disclosure to confirm that they have read and understood the policies/procedures.

Further information about compliance with the GDPR which is relevant to this case can be found at the following links:

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

<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/security/>

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

We would ask that the above changes be implemented as soon as possible, and in any event by 2 April 2020. We also request that you contact us on 2 September 2020 to update us on the changes you have implemented and any other measures you have implemented to improve your compliance with the GDPR.

Whilst the above measures are suggestions, we would point out that if further information relating to this subject comes to light, or if further incidents or complaints are reported to us, we will revisit this matter and further formal regulatory action may be considered as a result.

We actively publicise our regulatory activity and outcomes, as this helps us to achieve our strategic aims in upholding information rights in the public interest. We may publish information about cases reported to us, for example where we think there is an opportunity for other organisations to learn or where the case highlights a risk or a novel issue.

Therefore, we will publish the outcome of this investigation to publicise our regulatory authority and new powers under the GDPR. This will be in accordance with our Communicating Regulatory and Enforcement Activity Policy, which is available online at the following link:

https://ico.org.uk/media/about-the-ico/policies-and-procedures/1890/ico_enforcement_communications_policy.pdf

We will not name either the School or [REDACTED] when we publish the reprimand as we understand that the child still attends the School and we are aware of the concerns that would raise.

Thank you for your co-operation and assistance during the course of our investigation. We now consider the matter closed.

Yours sincerely

[REDACTED]
Lead Case Officer
Information Commissioner's Office
Direct dial: [REDACTED]

You should be aware that the Information Commissioner often receives requests for copies of the letters we send and receive when dealing with casework. Not only are we obliged to deal with these in accordance with the access provisions of the data protection framework and Freedom of Information Act 2000, it is in the public interest that we are open and transparent and accountable for the work that we do.

Please say whether you consider any of the information you send us is confidential. You should also say why so that we can take that into consideration. However, please note that we will only withhold information where there is good reason to do so.

The ICO publishes the outcomes of its investigations. Examples of published data sets can be found at this link: <https://ico.org.uk/about-the-ico/our-information/complaints-and-concerns-data-sets/>

For information about what we do with personal data, see our privacy notice at www.ico.org.uk/privacy-notice