DATA PROTECTION ACT 2018 AND UK GENERAL DATA PROTECTION REGULATION

REPRIMAND

The Information Commissioner (the Commissioner) issues a reprimand to Parkside Community Primary School (Parkside) in accordance with Article 58(2)(b) of the UK General Data Protection Regulation (UK GDPR) in respect of certain infringements of the UK GDPR.

The reprimand

The Commissioner has decided to issue a reprimand to Parkside in respect of the following infringements of the UK GDPR:

- Article 5 (1)(f) which states 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 or organisational measures ('integrity and confidentiality').

There are also infringements of Article 24 (1) (Responsibility of the controller) and Article 32 (Security of processing).

The reasons for the Commissioner's findings are set out below.

The investigation found that Parkside inappropriately disclosed personal data, including special category data, of a sensitive nature in a classroom environment. There were four data subjects affected, three of whom were children.

The Commissioner considers that in relation to the infringement of Article 5(1)(f) (and by extension Article 24 (1) and Article 32), that Parkside did not have adequate:

- Policies. The ICO is satisfied that the both of the employees concerned acted in contravention of Parkside's data protection policies by failing to report the breach internally. However, shortcomings with Parkside's policies were noted. Specifically, the data protection policies did not outline the course of action for employees to adopt to ensure security and confidentiality when sharing personal data internally by email and also when it was appropriate to open emails which contained personal data. This is particularly pertinent due to the classroom environment which Parkside employees operated in.

Also noted was a lack of policy relating to [redacted] ([redacted]). [redacted] is a case management system specifically used for the management and monitoring of safeguarding, wellbeing and pastoral issues related to children. The personal data being processed by [redacted] was likely to be sensitive and contain special category data, so the ICO would expect a controller to have adequate technical and organisational measures around the use of [redacted] to prevent a security breach.

- Procedure and guidance. There was a lack of written guidance for employees in respect of using security and confidentiality classifications on emails. Specifically and in relation to this incident, it was noted that emails generated by [redacted] did not have any security classification or labelling to indicate they contained personal data of a sensitive nature (including special category data).

  Further, there was no written procedure or guidance for employees in respect of when it was appropriate during the school day to open emails generated by [redacted].

  In addition to this, there was no written procedure or guidance available to employees in relation to the safe operation of the electronic whiteboards, particularly when screensharing from an employee's electronic device.

<u>Mitigating factors</u>

In the course of our investigation we have noted that:

- Parkside had overarching data protection policies in place. In particular, Data Protection and Security Policy (dated July 2020) stipulated that employees should follow the security incident / data breach response plan if they know or suspect a personal data breach has occurred. The Data Breach Response Plan Parkside Community Primary School (undated) directed employees that if they become aware of a suspected or actual personal data breach, then the incident should be reported to the Headmaster without delay.

- Once the incident was discovered by Parkside, the children who witnessed the disclosure were reassured that what they read was unfortunate and that if they wanted to talk about the content that they were able to do with the Deputy Headteacher. It was stressed to the children that the content was not to be discussed with their peers. There is no evidence that the disclosed [redacted] content has been shared or disseminated.

- Parkside referred the incident immediately to the Local Authority Designated Officer (LADO) and followed the recommendations made by the LADO.

- Chair of Governors agreed with commissioning the Human Resources team at Herts for Learning to carry out an investigation and it was conducted under the school's disciplinary policy.

- Formal disciplinary action was taken against one of the employees concerned. This employee made a statement of apology for breach and for their failure to report the incident.

Remedial steps taken by Parkside

The Commissioner has also considered and welcomes the remedial steps taken by Parkside in the light of this incident. In particular we have noted that:

- The governor responsible for the strategic management of UK GDPR reviewed the Parkside's current practices in line with the Data Protection policy and made recommendations to the full governing body.

- All staff were issued with a formal notice and guidance about how incidents should be reported on the school's interna[redacted].

- New guidance has been issued to staff around the recording and accessing of work emails / [redacted] records in light of the breach.

- Staff have been instructed that all alerts sent via[redacted] are only to be read at specific times of the day and never when children are present or in the vicinity of the classroom.

- All staff have been instructed to use "SENSITIVE/HIGHLY SENSITIVE" in the subject line of an email informing the recipient of the nature of the content before it is opened. Such emails should only be read before and after the school day.

- Governors are to be alerted to an incident as soon as it becomes known to the headteacher.

- Cases of a complex and sensitive nature can only be accessed on [redacted] by the Headteacher, Deputy Headteacher and Parental and Pastoral Officer and shared with relevant members of staff on a need-to-know basis at scheduled meetings.

- All staff and governors received UK GDPR refresher training (which included the caveat not to check emails during teaching time) as per the Herts for Learning training module. Part of the training instructed staff to use the internal secure data transfer system when sending information of a highly sensitive nature.

- All staff to be issued with the Parkside's UK GDPR policy and to be familiar with its content. A record will be made on personnel files in this respect.

- Staff have been signposted on where to access the school's Data Protection Policy as a point of reference should they require it.

- Parkside's Data Protection Policy has been reviewed and an appendix added for review at the first full governing body meeting of the new academic year. The updated policy instructs staff how to report a breach, what constitutes a breach, who to report it to and what happens once this has been do. This is to help staff understand the complexities of reporting a breach.

- All staff to sign an electronic document to say they have read and understood the school's Child Protection and Data Protection Policy in September 2022 alongside the latest and updated version of Keeping Children Safe in Education (Part 1).

Decision to issue a reprimand

Taking into account all the circumstances of this case, including the mitigating factors and remedial steps, the Commissioner has decided to issue a reprimand to Parkside in relation to the infringements of Article 5(1)(f), Article 24 (1) and Article 32 of the UK GDPR set out above.

Further Action Recommended

The Commissioner recommends that Parkside should take certain steps to ensure its compliance with UK GDPR. With particular reference to Article 5(1)(f), Article 24 (1) and Article 32 of the UK GDPR, the following steps are recommended:

1. Parkside should consider refresher training on the operation of electronic whiteboards for all relevant employees. This should be underpinned by written guidance for employees to follow and Parkside should satisfy itself that security is enshrined in the training and guidance. Emphasis should be given to the relevant steps for employees to take to avoid a personal data breach when operating an electronic whiteboard.

2. At the time of the breach, it was noted that there was no written guidance in place for employees for the use of [redacted]. Whilst it is appreciated that Parkside have now issued some written guidance in relation to the operation of [redacted], Parkside should evaluate whether this is sufficient and adequate to reduce the risk of a recurrence of a similar incident. [redacted] refresher training should also be considered for all relevant employees.

3. Consideration should be given to refresher data protection training to all members of staff, as it was noted that both members of staff involved in this incident failed to report the breach. Emphasis should be given on the requirement to report a suspected or actual personal data breach. Parkside should satisfy itself that all employees understand the consequences of failing to report a breach, particularly as it can mean a delay in mitigating action being deployed. This is especially important, as mitigating action can lessen the effects of a personal data breach and the potential impact on the data subject/s.

4. Parkside should satisfy itself that it has adequate technical and organisational measures in place to ensure the security and confidentiality of emails sent internally which include personal data, particularly when these contain sensitive or special category data.

5. Parkside's policies and procedures should have prominent, sufficient and adequate practical guidance for employees in order to avoid a similar breach occurring again. This also needs to include regular reviews, and proactive work to increase staff awareness of these.

6. Parkside should take steps to test all of the new processes introduced as a result of this incident and ensure they are embedded within the organisation.