-

GDPR and COVID-19

(WORKING REMOTELY)

Policy Owner	**Applies to**	**Superseded documents**
PPS Governing Body	Prior Park Schools (Trust Wide)	NA
Associated documents PPS GDPR Data Protection Policy Schools own Remote Learning Policy	**Review frequency** NA **Implementation date** 24 March 2020	**Legal Framework** General Data Protection Regulations Data Protection Act (DPA) 2018

1. Introduction

Prior Park Schools (PPS) comprises three schools. Two of those schools, Prior Park College and The Paragon School are incorporated in England as Prior Park Educational Trust Ltd. The third school, Prior Park School Gibraltar, is incorporated in Gibraltar as Prior Park School Ltd. Both are companies limited by guarantee and registered charities.

2. Scope

This extension to the PPS GDPR Data Protection Policy should assist all PPS staff whilst working remotely (e.g. from home) during this period of 'lockdown'. This extension must be used in conjunction with the PPS GDPR Data Protection Policy.

It is acknowledged that during this period of remote working PPS staff will be continuing to work with student, parent and staff Personal Data, but that this will, most likely, not be in their school office. To ensure PPS is GDPR compliant, all staff must follow the below guidance (section 3) to ensure any Personal Data is kept safe and secure. Therefore, all staff will adopt physical, technical, and organisational measures to ensure the security of personal data. This includes the prevention of loss or damage, unauthorised alteration, access or processing, and other risks to which it may be exposed by virtue of human action or the physical or natural environment. A summary of the personal data related security measures is provided below:

- Prevent unauthorised persons from gaining access to data processing systems in which personal data are processed.
- Prevent persons entitled to use a data processing system from accessing personal data beyond their needs and authorisations.
- Ensure that personal data in the course of electronic transmission during transport cannot be read, copied, modified or removed without authorisation.
- Ensure that access logs are in place to establish whether, and by whom, the personal data was entered into, modified on or removed from a data processing system.
- Ensure that in the case where processing is carried out by a data processor, the data can be processed only in accordance with the instructions of the data controller.
- Ensure that personal data is protected against undesired destruction or loss.
- Ensure that personal data collected for different purposes can and is processed separately.
- Ensure that personal data is not kept longer than necessary.

3. What does this mean for me?

All PPS staff are required to;

- Only in exceptional circumstances should any paper files which include Personal Data be taken from any PPS school site. Permission to do so is only with the agreement of the Head. Each case will be view on the reasons why it is imperative to have this paperwork.

- Ensure that any calls are made via the Teams App whenever possible. Only in exceptional circumstances should staff be calling students or parents on their own phones. However, it is accepted that during this 'lockdown' phase there are sometime no other alternative. Staff should use the 141 dialling facility before making calls to ensure their Personal Data isn't stored by any students or parents, and staff should also ensure they do not store any mobile numbers for students or parents on their own phones.

- Ensure all paper files are kept safe and secure when not being used e.g. in a lockable cupboard/drawer.

- Ensure that when paper files are being used, they are done so in a secure and safe environment e.g. home office safe.

- Ensure that no members of the household have access to paper files.

- Ensure that all sensitive electronic files (e.g. those containing Personal Data) are only downloaded/used on a PPS electronic device.

- Ensure that when these electronic devices are not in use they are 'locked' with a password protection function.

- Ensure that these devices are securely stored when not in use.

- That all records are securely and correctly destroyed when no longer needed e.g. shredded when available or safely secured to be shredded upon returning to a PPS school.

- Ensure that all paper files are safely and securely returned to their respective PPS school upon lifting of 'lockdown'.

- Ensure that all correspondence to students, parents and staff are made using the agreed systems e.g. SchoolBase/Teams and/or Prior Park Schools email accounts

4. Reporting a Breach

Any individual who suspects that a Personal Data Breach has occurred due to the theft or exposure of personal data must immediately notify;
Emma Wickham (ewickham@priorparkschools.com) providing a description of what occurred. Notification of the incident can be made via e-mail.

Any Data Breach will be investigated, and confirmation will be sent as to whether or not a Personal Data Breach has occurred. If a Personal Data Breach is confirmed, they will follow the relevant authorised procedure based on the criticality and quantity of the Personal data involved. For severe Personal Data Breaches, Prior Park Schools Leadership Team will initiate and chair an emergency response team to coordinate and manage the Personal Data Breach response.