Alpha Plus group
the Gold Standard in education

FALCONS PREP
RICHMOND

# GDPR and Data Protection Policy

| |
|---|
| **Primary person responsible for this LINK:** Tania Gomes |
| **Job title:** Head's PA, School Administrator & GDPR Co-ordinator |
| **Created:** June 2020 |
| **Next review date:** June 2021 |

# DATA PROTECTION POLICY & PRIVACY STATEMENT LINKS

**PLEASE CLICK ON THIS LINK FOR THE APG DATA PROTECTION POLICY:**

https://egiportal.alphaplusgroup.co.uk/Alpha%20Plus%20Group%20Information/Data%20protection/Alpha%20Plus%20Group%20Data%20Protection%20Policy.pdf

**PLEASE CLICK ON THIS LINK FOR THE APG EMPLOYEE PRIVACY STATEMENT:**

https://egiportal.alphaplusgroup.co.uk/Alpha%20Plus%20Group%20Information/Data%20protection/Alpha%20Plus%20Group%20Employee%20Privacy%20Notice.pdf

**PLEASE CLICK ON THIS LINK FOR THE APG PUPIL & PARENTS PRIVACY STATEMENT:**

https://egiportal.alphaplusgroup.co.uk/Alpha%20Plus%20Group%20Information/Data%20protection/Privacy%20Policy%20for%20Students%20and%20Parents.pdf

**PLEASE CLICK HERE TO VIEW THE DATA RETENTION POLICY:**

https://egiportal.alphaplusgroup.co.uk/Alpha%20Plus%20Group%20Information/Data%20protection/Alpha%20Plus%20Group%20Data%20Retention%20Policy.pdf

## 1. PLEASE FIND BELOW IMPORTANT DATA PROTECTION FAQ's FOR YOUR CONVENIENCE:

### What happens if I lose my mobile or surface pro?

As most of us can access our emails from our personal mobile phone this is a clear breach under GDPR. Any loss of a mobile, surface pro or USB pen must be reported immediately to your DPO Mrs Gomes. Please be prepared to inform Mrs Gomes of what sort of data you had on the device and what could be accessed due to not being password protected.

### What if I send an email to the incorrect person?

If the email does not contain any personal data you would only need to apologise for sending it incorrectly. However, if the email does contain personal data this is a clear breach under GDPR and must be

reported to your DPO – Mrs Gomes immediately. This must be followed by an email to the receiver requesting them to please delete the email and not share any information.

## What constitutes 'personal data'?

Personal data relates to a living individual who can be identified either from the data or from the data in conjunction with other information - for example a name plus a telephone number, address, date of birth, email address, photograph, and so on. Personal data also covers written comments about an individual e.g. a teacher's comment about a student in a professorial report and in general email correspondence.

## What is Data Subject Access Request?

Right of Access, also known as a DSAR gives individuals the right to obtain a copy of their personal data being processed by a Controller as well as other supplementary information. This 'Right of Access' helps individuals to understand why and how you are using their personal data.

An organisation who has been issued with a DSAR has one calendar month from the date it is received to provide information to the individual. Where the controller requests identification from the individual then the date would start once the identification has been provided. For practical purposes, if a consistent number of days is required (e.g. for operational or system purposes), it may be helpful to adopt a 28-day period to ensure compliance is always within a calendar month.

A request can be made in writing or verbally and can be made to any part of an organisation (including via social media) and it does not have to be addressed to a specific person or contact point. A request does not have to include the phrase 'subject access request', as long as it is clear that the individual is asking for their own personal data.

## What are the 7 GDPR data protection principles?

Data protection laws across the globe have always had at their heart core data protection principles. GDPR specifically stresses the requirement for organisations to be accountable. The seven principles are:

1. Lawfulness, Fairness & Transparency
2. Purpose Limitation – be clear about the purpose(s) you will use personal data for
3. Data Minimisation – only collect the personal data you need for your clear purpose(s)
4. Accuracy – personal data should not be inaccurate or misleading
5. Storage Limitation – don't keep personal data for longer than you need it for your clear purpose(s)
6. Security – ensure appropriate security measures are in place to protect personal data
7. Accountability – you must be able to demonstrate your commitment to all of the above.

## What is a privacy notice and where should they be displayed?

A privacy notice is a public statement of how Alpha Plus Group applies data protection principles to processing data. It should be a clear and concise document that is accessible by individuals.
At every point where data collection happens there must be a privacy notice or statement. For example; when you send forms out to parents requesting information there must be a clear privacy statement or a link to the APG privacy notice, which can be found on the APG website.
We advise that for all forms you add the link to the group privacy notice.

## Is it ok for students to sign up for extracurricular classes and other departmental activities via noticeboards?

Yes, this is fine as the student is selecting a class/activity and merely signing up. Once the list is no longer required it should be destroyed.

## Am I allowed to take documents on a USB home to work on them?

This is a risk owing to the fact that a USB could be lost. If there is personal data on the USB, this would be a clear breach under GDPR.

All staff have access to Microsoft OneDrive, cloud storage for files from home via VPN, both of these options mean that taking a USB home to work is unnecessary. Contact the IT Department if you need any assistance with this.

## One of the teachers in my department has asked me to log into their APG email account to retrieve their monthly payslip. Am I allowed to do this?

No - this is a breach of the APG IT policies and data protection. Staff should not share their log-in details with other colleagues and should be using their APG email themselves.

## Will we be allowed to take a copy of invoices from casual teachers or staff time sheets in case we need to chase payment with Finance?

It is ok to take a copy as long as it is not retained for longer than necessary (i.e. once the payment has been made). In practice though, ask yourself how often you actually need to chase payments (and specifically) provide a copy of the documentation again?

## Do I need to delete emails that have personal information in them or in attachments (like student application forms)?

Yes - It is good practice under current Data Protection regulation to delete anything containing personal information unless there is a good operational reason to keep it for a specified period. Where you are keeping an attachment in an email for future reference it is

good practice to save the document on a secure system and delete the email (see the APG Retention schedule for more details).

## What happens if I lose my personal notebook?

Personal notebooks strictly speaking wouldn't usually be covered by the GDPR. This being said sometimes you may collect sensitive or confidential information within your personal notes. If you feel this information would be damaging to an individual, if it was lost, then it's always advisable to report the loss of them to your DPO Mrs Gomes. It is also advisable to destroy notebooks once they are no longer required.

## How do I know how long I need to keep data for?

Alpha Plus Group has issued a new Retention Policy. This policy will detail how long all information should be kept for. If you are unsure or feel the policy misses something, then contact head office via DPO@alphaplusgroup.co.uk

## I use social media for work, how does the GDPR affect me?

When using social media to share information (such as photos or videos) on data subjects, always make sure you gain consent of the individuals and can remove information upon request.

## Can I keep using school photos after a pupil has left?

If you have gained and recorded consent, and it is clear that photos will be kept after a pupil has left then this is fine.

## Can I use Whatsapp?

The use of any technology outside of the issued tools is not allowed and should not be used for official work purposes. Keep personal apps and tools for personal use only.

## Can a parent or pupil request their data (SAR) verbally or do they have to go through the Alpha Plus process?

Individuals can request information in any way they see fit. This can be verbally, in writing or electronically. Alpha Plus have a process which we will always guide individuals to follow however data subject do not have to follow this process.

## Can I share parents' details with other parents?

Yes, if the parents are aware of who their information will be shared with and that they have given consent for their information to be shared.

## Can I use parents or students data to contact them for non-Alpha Plus business purposes?

No. This is unlawful under the GDPR & DPA 2018. Any employees using personal data inappropriately can be directly prosecuted and fined by the ICO.

## What should I do if an organisation, such as the police or social services, requests information on one of our parents or students?

Care must always be taken to ensure that the sharing of personal data is done so lawfully and securely. In all cases, before you share data with any 3rd parties, you should contact the DPO (DPO@alphaplusgroup.co.uk ) to ensure the activity is allowed.

## Can I take photos at events with parents for marketing and promotional purposes?

If you are running an event, inform attendees at the start and ask them if they are ok with photos being taken. Most event organisers give a visual key on a tabard of some sort to show those that don't want their pictures taken and delete those pictures where they are captured. Also, you can designate areas and times where photos are taken and make people aware so they can avoid those areas if needs be. If the event is in a public area then you have free reign to photograph whoever you want.

## Secure destruction of paper based records

All paper records containing personal information should be destroyed securely. As a minimum they should be shredded. If the document contains confidential or sensitive information then measures should be taken to ensure the secure destruction of those documents.

## Is there any basic guidance online that I can access?

Yes, the Information Commissioners Office (ICO) who has responsibility for enforcing GDPR in the UK has a range of guidance for organisations. This provides a useful overview of the basics in terms of what you need to do now:
https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf

## Can a parent apply under a 'subject access request' to see anything written about a child (including references)?

Schools have an obligation to recognise such a request. Any data provided must have other names redacted, especially if it refers to staff or other pupils. If parents specifically ask to see a references, we tell them they can ask the recipient school for it (pointing out that it is best not to ask for this until they have heard from the school) and leave it up to them to share or not.

## Do we need consent when seeking/providing student references?

Where schools or colleges require pupil references from previous schools and intend to contact those schools directly, they must make this clear on their application forms and obtain the signed consent of the parents to do this. The application forms and the school's admissions policy should make it clear where failure to consent to this or to provide these references by alternative means may affect

the pupil's application, or even refuse to admit pupils without it if they choose.

Where requests are received by our schools from a pupil's future school to provide a reference, these should not be given without our having obtained prior written permission of the parent (or pupil where over 13 years of age). This can be obtained on a standard form before the pupils leave our schools or on a case-by-case basis.

The only exception to the above will be EHCPs which have to be passed on between SENCO officers from school to school.

If, as is particularly the case with international pupils attending colleges, pupils personally ask within 12 months of leaving for a reference from us by means of written evidence of attendance, copies of lost reports or copies of exam certificates then as long as suitable ID is provided it is reasonable to provide this. Requests for this or any other information beyond 12 months after leaving date are best treated as a DSAR and recorded as such.

It is vital that any references we provide containing special category data, such as SEN or medical data, are sent securely using encryption or suitable postal arrangements.

Pupils will often at some point in their lives ask for a character reference from a member of staff, but these will be personal references and as long as this is made clear to the recipient they are not affected by the above rules.

### Do we need to obtain permission from staff members for them to be included in public documents such as policies and student handbooks?

No, this forms part of staff's contractual obligations for their details to be used in policies and documents. We do however advise that you do make staff aware anytime when their details may be made public and searchable.

## 2. Distance Learning and Working from Home

Questions to consider

· Where you plan to use new tools, have you checked that they are GDPR-compliant and whether consent is needed from parents/pupils (contact dpo@alphaplusgroup.co.uk for advice)? · Have staff been reminded about the importance of data protection / relevant APG policies when working from home?

**Guidance**

a) Recording videos calls: If schools plan to record video calls, they should be clear about the purpose. Schools should consider recording video calls with pupils as a precaution. Where safeguarding is the sole purpose for recording, parents and pupils should be kept informed about the practice, but our Data Protection Officer has advised that consent is not required. If schools also plan to distribute recordings (e.g. if they plan to send recorded live lessons to those who missed a class1) this should be made clear to parents and pupils and consent should be sought. Schools should check the wording in their image/video consent forms sent out at the start of the year as they may already be covered. If concerns are expressed about recording and/or distributing video calls, staff may allow a pupil to mute their microphone/turn off their webcam where appropriate so that they are not included in any recordings. Recordings should only be shared as required and for as long as needed. Staff/pupils/parents must not share the recordings more widely.

It is recommended that any recordings are saved to Microsoft Stream and kept for a year to allow time for any safeguarding concerns to be raised. The recordings should then be deleted. If calls are recorded in Teams then they will automatically be uploaded to Microsoft Stream and will be made available to those who were in the call as default. Permissions can be added or removed by the staff member as needed. For recordings captured outside of Teams (e.g. in Zoom) the video should be recorded to the local device and then uploaded to Stream. Staff must ensure that permissions are set correctly when uploading to ensure the video isn't shared with the entire organisation (see guidance on setting permission here. Local copies should be deleted once uploaded. Additional guidance on using Microsoft Stream can be found here; please speak to your IT engineer for further support.

Please note that Stream videos cannot be shared externally, where this is required you might consider hosting videos on platforms such as Private YouTube Channels or Estream. Please check that the platforms you choose are GDPR compliant (you can contact dpo@alphaplusgroup.co.uk for guidance). b) Working from home: staff must continue to follow APG's data protection policies. In particular, staff must continue to keep personal information secure and must report breaches and subject access requests to dpo@alphaplusgroup.co.uk. Staff should avoid storing files on personal workstations and should continue to save them within their school systems. Strong passwords should be in place and data encrypted if a USB stick is used. Staff are reminded to not leave a device unattended when logged in and to not download or open any suspicious content.