Archers Brook SEMH Residential School

Working from Home Policy for Staff

Archers Brook SEMH Residential School

Working From Home Policy

Review Date	Changes Made	By Whom
May 2019	Policy format and content updated in line with CWAC changes	June Sedgwick

Background

Taking work home is generally considered to be an informal arrangement and there tends to be an expectation that staff will at some point take work home with them.

Archers Brook has a responsibility to ensure that it takes the appropriate steps to ensure that any personal data relating to staff or pupils that is removed from the school environment is treated in an appropriate manner. Archers Brook has developed a written procedure (below) which clearly sets out what can be removed from the school premises and how it should be handled. All staff will be made aware of this procedure and sign to confirm they understand.

Does GDPR mean we can't work from home?

GDPR is not that prescriptive in its requirements. What GDPR and all data protection legislation requires you to do is to ensure that you handle and treat personal data appropriately and the key principle here is to ensure that data is handled and kept securely. So while it is up to the school's discretion in terms of what they allow, they must take steps to ensure they maintain an appropriate level of security for any personal data used off site.

What do we (Archers Brook) need to consider?

Archers Brook will consider a number of issues for this homeworking policy specific to your school:

- The nature of Staff – this will Govern the nature of the information AB will be happy for Staff to take off premises to work on. For example, AB may happily identify there is minimal risk in teachers taking work home to mark due to the low level nature of personal data, but if a member of office staff is allowed to take work home, does this involve a greater amount of personal data – for example pay roll information. So think about who can work from home and what they may be doing.
- The nature of the information involved – again, a lot of the items a teacher may take home to work on will contain minimal personal data if, for example, it is work to mark. But there may be occasions where they have access to a lot more personal data – for example when completing reports etc. Again, staff who work in the office and may have access the personnel files may handle a lot more personal data, so think about what – if anything - you are happy for them to remove to work on at home
- It is not just paper files – Archers Brook have to consider what we are happy for staff to access from home. Can they log into the school's system either on a school or personal laptop?. If so, what security measures are in place, do staff know they cannot download information and save it locally to their own PC etc.
- Home security – all information should be secured at night. It should be locked away and staff/governors remain responsible for the security of information at all times.

- Transporting information – paper files must be carried in an appropriate bag, if a member of staff needs to information home. An encrypted USB supplied by the school must be used where information is downloaded.
- Staff (including Governors) should use their school email accounts (to send work home or to school etc) and personal accounts should not be used. Where school business is involved, information held in personal accounts is still subject to Freedom of Information requests and Right of Access (Subject Access Requests) Requests and staff would have to comply with requests for such information. Where staff may be unavailable and information is held in personal accounts, this may restrict our ability to service the requested in the required timescale.

Working from Home Policy

Personal data held in physical documents taken home by staff must be kept secure.

Take steps to ensure the security of these documents and keep data safe, to avoid a data breach and stay compliant with the GDPR.

Under the General Data Protection Regulation (GDPR), you should be doing everything in your power to prevent a breach of personal data.

This includes ensuring that any physical documents containing personal data taken home by staff are kept secure, to prevent the data from being lost, stolen or accidentally leaked.

There are no specific rules on how you must do this, but you can take the practical measures below, you may also want to introduce additional measures at your own discretion.

Store data remotely, where possible

As far as possible, keep personal data in an electronic format on a server that staff can access remotely when working from home.

Ensuring this data is stored remotely means it can't be misplaced or lost.

Documents with little personal data, such as student work books or coursework or planners, are suitably low risk these items are allowed to taken home by staff. This is also practical, as it allows teachers to mark work more easily.

Documents with more substantial amounts of personal data need more scrutiny in how they're handled. These include:

- Pupil records
- Annual or termly pupil reports

However, you should consider the practicality of preventing staff from working on documents at home. Consider remote access arrangements, as noted in the section above. Only on rare occasions should staff take any personal data/documents home, ie meeting in morning and needing to go directly from home.

If documents/information in regard to a pupil are/is copied for a meeting, staff need to account for the information ie if 5 copies printed and 2 copies are handed out and kept by a Social Worker/Professional then the other 3 copies need to be shredded.

Sign out procedure

If staff are removing documents with significant amounts of personal data that are held by a central office, such as pupil records, they should be made to sign out the records and sign them back in once they have been returned.

This ensures that you know who holds the documents at all times, and it will remind staff of their responsibility to prevent the documents from being lost or stolen.

Staff must keep documents in a secure file.

Documents should be kept in a closed folder, such as one with a zip lock. Staff should include their name and contact details in case the folder is lost.

Secure Place

Staff should place the documents in a secure area of their house. Staff should keep documents somewhere specific, such as a certain drawer or tray, to prevent them from being lost.

In particular, staff should avoid leaving documents in their car, as this creates a higher risk of them being stolen.

When returning the documents to school, staff should take them immediately to their original storage place rather than leaving them on desks to return later.

How to make devices secure

Staff are supplied with encrypted devices. It's easier to ensure that devices used to process personal data have a suitable level of security when supplied to staff members directly.

IMPORTANT

Keep the device password-protected
Use a strong password or a PIN to lock devices, to prevent others from accessing data through them.

Strong passwords are at least **8 characters**, with a combination of upper and lower-case letters, numbers and special keyboard characters (e.g. an asterisk or currency symbols).

Google has further advice for users on how to create a strong password. These include:

- Replace letters with numbers and symbols. For example, replace ‘a’ with ‘4’
- Don’t use personal information such as pet names or nicknames
- Don’t use common words (e.g. password) or sequences like 1234
- Don’t reuse passwords

If a wrong password or PIN is entered too many times, access to the device should be locked, or data stored in it should be automatically deleted.

Encrypt the device

If personal data is stored on a device or likely to be, ensure that the hard drive is encrypted.

Encryption means the data is converted into a code and can only be converted back using 'the key' (such as a password). Only users with the key will be able to read it.

This means that if the device is lost or stolen, someone cannot access the files stored on its hard drive by attaching the drive to a new device.

Signed: ……..
Mrs Myers-Whittaker
Headteacher

Date: .....……

Signed: ……..
Mr R Crompton
Chairman of Governors

Date: .....……