

COVID testing in school - Data protection risks and mitigation

Schools and Trusts have been expected to prepare for COVID testing of staff and students with very little notice. As part of this testing you are required to gather and process additional personal data from the test subjects (both staff and students). Some of this is **special category data** which requires additional care when handling. During this important task, it is essential that throughout the process any personal data is handled appropriately and in line with data protection regulations. Please share and discuss these risks with all staff involved in the testing process.

Personal Data required during the testing process

- Name
- Date of birth (and year group)
- Gender
- **Ethnicity (special category data)**
- Home postcode
- Email address
- Mobile number
- Unique test barcode/number
- **Current COVID status or symptoms (special category data)**
- **Test result (special category data)**
- Parent/guardians/carers contact details (if required)
- Relationship to test subject
- Signature

Key risk: Inexperienced staff do not handle sensitive personal data appropriately

All school staff should have up-to-date data protection training. Remind staff that all personal data should be kept securely, shared with others only where essential to the process, never left out in public view. Online data protection training is available for any new member of staff or any staff who requires refresher training.

Key risk: Valid consent is not held before testing occurs.

The process includes checking consent is held before the testing is carried out. Data subjects can opt out at any stage. Where the test subject is under 16, if there is any question about the consent being held and valid, a test should not be carried out before the parent is contacted to verify consent.

Key risk: Documents are left on show in the registration or recording desks

Documentation should be kept electronically where possible. Desks should be orientated so data subjects cannot read the screen when it contains personal data of another person. If consent forms are held on paper they should not be left in view of other data subjects. Devices must be locked or shut-down when not in use or unattended at any time. Desks must be cleared at the end of each testing session and any documents secured. Also brief support staff in case any documents are found during cleaning.

Key risk: Results are shared with the wrong recipient or their parent/carer

Staff involved in contacting parents or students informing them of a positive test result should be careful to match the contact details provided on the consent form to any other contact details held in the schools MIS systems. Date of Birth should be matched as well as name in case of similar names.

Continued



Key risk: The portable devices used to scan barcodes store information about the tests in the browser cache.

It is recommended that only school devices are used to scan barcodes and input data into the NHS testing website. It is also recommended that web browsers are used in 'private' or 'incognito' mode which ensures that no data is stored from the browsing session on the local device, once the browsing session window is closed. Browser sessions must be closed at the end of each testing session. Devices must be locked or shut-down when not in use or unattended at any time.

Key risk: Test documentation and registers are shared with all staff

Any documentation, either electronic or paper, must be stored securely with restricted access by only staff involved in the testing. If kept electronically the register must not be stored in an '**all staff**' area of the school system, where potentially staff not involved in testing could access and look up the test results of someone else. The spreadsheet should be password protected and/or held in a restricted area with limited access.

Any paper documents including consent forms must be stored securely.

Key risk: Identity of a positive test subject is shared with close contacts

When informing close contacts it is important that the identity of the person with a positive test remains anonymous. If they choose to inform their friends or colleagues directly that is their choice but the school must not inform anyone else on their behalf without valid consent.

Key risk: Staff informing parents of a positive test are overhead in school office

It is important that staff make phone calls in an area where they cannot be overheard when informing parents or students of a positive test and the need to return home and isolate.

Key risk: Test results are discussed amongst staff

It is essential that any staff handling both consent forms and test results respect that they are highly sensitive personal data. Only essential staff should be given access to test results, they must not be discussed publicly amongst staff.

What to do if a breach does occur.

Inform your COVID-19 coordinator or school business manager who will work with the DPO to investigate the breach and deal with it accordingly.