COVID-19 Preparation for Schools

Data Protection Frequently Asked Questions

This guidance is for schools who are planning for potential closures and disruption to children's learning.

As schools consider different ways to deliver learning and support pupils, it is important that they **still follow the principles of data protection legislation**. This will not be a barrier to learning, but schools must check with their Data Protection Officer before sharing pupil and staff personal data in any new ways, or with any new service.

Key considerations

Access and permissions

- In the event of staff illness, can school business continue? If only one staff member has administrator access, extend permissions to other key staff on a temporary basis. Document changes made and review at the end of the current crisis.
- Ensure that a copy of administrator passwords for government services is held in the school safe, not just with the headteacher.

Physical Security

- Do a key audit – where are all your keys, and how will you manage if a keyholder is unwell?
- If the school is closed, ensure that all sensitive pupil and staff data is securely locked away.
- Ask all staff to lock away any personal data they hold – avoid staff taking physical copies of pupil personal data home for the duration of the closure, in case of staff illness.
- If staff do take data off-site, keep a full record of what they have taken, and remind them of the school security policy (see FAQs).

Technical Security

- Check with your school technician – will all systems perform in the event of a sustained closure? Is any essential maintenance likely during the closure?
- Is statutory school data being backed up to your main systems, and if not, how will this be managed?
- Has the technician shared any necessary passwords in the event of their own illness?
- Audit staff laptops – how many do you have, who has them, is their anti-virus up to date?
- Consider how you will manage password resets for school services.

Frequently asked questions

We want to set up a new online learning tool – can we do this now?

- Contact your Data Protection Officer, as they may have dealt with other school queries about the tool.
- Any online learning tool must be carefully considered, but a Privacy Impact Assessment will only be required if high levels of pupil personal data are being uploaded (e.g. full names, classes, gender, contact data).
- If only pupil first names and classes are being uploaded, this is not high risk.
- In any event, only upload the minimum pupil data actually required by the tool.
- If the tool is taking data from SIMS, check that it (or an integrator such as Wonde) is only taking the minimum data it requires to provide the service.
- Inform parents that you are planning to use the tool – you do not need to ask for their consent (your lawful basis is Article 6(1)(5) Public Task) but you do need to inform them that the tool is being used with learners. We must consider any objections from individual parents and provide offline alternatives if possible.
- Trial the tool with a class first, then extend across the school when you are confident that the system is secure and effective.
- Consider how you will manage passwords if the school is closed – how will students/staff get their password reset?

Staff will be working from home – is our data safe in their home office?

- Remind staff of the appropriate sections in your Data Protection policy – Staff Responsibilities and Data Security.
- The same policy applies in the event of home working – if using a computer/laptop for school business, they must be aware that family members do not have a right to see data about pupils.
- If they have remote access to the school server or a school portal, they must use this (or Office 365 OneDrive) rather than saving pupil data to their hard drive or memory stick This ensures that the school can still access the data in the event of a staff member falling ill.
- If you don't have remote working systems, check with your IT providers. Connections must be secure, to minimise the risk of ransomware attacks on school systems.
- The staff member must report any data loss, malware / ransomware attack or data disclosure to the school immediately.

We have a Subject Access Request that is currently underway – can we extend our response time if staff are unavailable?

- Yes – contact your Data Protection Officer. They will provide you with a draft letter to the data subject and support you with information gathering.

COVID-19 Preparation for Schools
Data Protection Frequently Asked Questions

What happens if a new request for data (a Subject Access or Freedom of Information request) comes in?

- Contact your Data Protection Officer. They will support you to acknowledge the request, clarify the data required by the requester, and set a realistic timescale for response.

Can we share information about affected learners with other schools e.g. where there are siblings?

- It depends what you want to share! The information shared must be necessary, proportionate and relevant – e.g. only share what you need to, when you have to.
- Parents should be asked for their consent, but if no consent is forthcoming or cannot be obtained, consider whether you can share the information without consent.
- Check with your Data Protection Officer - there is a lawful basis for sharing Special Category data (medical information) for public health reasons, but your DPO will need to know why you are sharing it without consent.
- Share securely, and with the right person at the other school. Keep a record of what you shared, when and with whom.

We want to communicate with parents – should we share staff email addresses?

- Staff communication with parents must be open, transparent and accountable.
- There are more effective and secure ways to manage communication with parents than emailing staff directly.
- Sharing staff email addresses puts staff under increased workload at a time when they may be unwell and is not effective for business continuity.
- It also increases the risk of a data breach if staff are emailing multiple parents or mis-filing essential emails.
- Consider setting up a new mailbox for learning questions e.g. homelearning@nameofschool.somerset.gov.uk or department mailboxes. Then set up a rota for staff to monitor the mailbox and respond to queries.
- Communication should be kept to learning / curriculum support, and discussions about pupil wellbeing should be minimised.

Contact and support

- Contact the eLIM DPO with any questions and requests for support dposchools@somerset.gov.uk
- Sign up to our monthly data protection newsletter here: https://us11.campaign-archive.com/home/?u=2ffddbefda06354a51a264e68&id=4d5776687c