

ITASS Data Security Guidance

Head Teacher's Data Security Guidance

This document is exclusively for Head Teachers to assist in the compliance of data security for schools. There are related key documents that require your attention for implementing, signing or understanding your duty and responsibility to implement data security in your school.

Data security

Things you will need to do to ensure effective data security policy

- Make sure all staff with access to personal data on children or vulnerable adults have enhanced Criminal Records Bureau (eCRB) clearance
- Appoint a Senior Risk Information Officer (SIRO)
- Identify information assets and for each one, identify an Information Asset Owner
- Conduct data security training for all users
- Put in place a policy for reporting, managing and recovering from incidents which put information at risk
- Shred, pulp or incinerate paper when no longer required
- Make staff and learners (and parents where applicable) aware of what data is being held about them and what it is being used for by issuing privacy or fair processing notices
- Make sure that, where appropriate, contracts for employment state that misuse of such data is a disciplinary matter.
- Store data security policies and guidance in a place that is accessible for all staff.
- Ensure staff have signed and understood an acceptable use policy that has reference to Data security

Senior Information Risk Officer

As the head teacher of the school you are responsible for appointing the **Senior Information Risk Officer (SIRO)**

The SIRO is a senior member of staff within the school who is familiar with information risks and the organisation's response.

The SIRO has the following responsibilities:

- Own the information risk policy and risk assessment
- Appoint the Information Asset Owners
- Act as an advocate for information risk management
- Disseminating guidance
- Ensuring policy compliance

Therefore it may prove worthwhile delegating a person with authority the responsibility of informing and training staff and making sure they are kept up to date.

What is an Information Asset Owner (IAO)?

This is a user who gathers information to create new data that contains personal information rather than just viewing data in its existing format.

Schools must identify their information assets including personal data. A model form is available.

ITASS Data Security Guidance

What are your responsibilities as an IAO?

- What information is held, and for what purposes
- How information will be amended or added to over time
- Who has access to the data and why
- How information is retained and disposed off

Knowing this information will enable you to manage and address risks to information and its handling and that it complies with the Data protection act.

Privacy Notices

To comply with the Data Protection Act, the school must issue a **Privacy Notice** document to the parent/carer of each pupil, and to the pupil if he/she is over 13 years old, and to each member of staff who is in scope of the School Workforce Census and for whom the school therefore needs to keep data in SIMS.

You should also issue the pupil Privacy Notice to pupils:

- At the start of the academic year in which they become 13 years old
- At age 16, when the right to opt out of passing information to Connexions passes from the parent to the child

The Privacy Notice document explains to the individual why the school collects data about him/her, who the data is passed on to (the LA and the DCSF), and where he/she can get more information.

Copies of the pupil and staff Privacy Notice documents are available to download from the ITASS website at <http://www.itass.newham.gov.uk/admin/manuals.aspx>.

What is an information User

This is a person who will use personal data but not make any changes to the way it has been supplied to them.

It is likely that most of your staff are information users and will need to be kept informed about data security and aware of how to handle information.

Accessibility to information kept on data security

All staff will need to be aware of the Data Protection Act, L.A. Guidance and School Policy on data security. Documents must therefore be kept in an accessible place.

Acceptable use policies

All staff will need to sign a hard copy of the acceptable use policy and confirm they are working within the policy on an annual basis. The recommended AUP is on the LGFL site and has been approved by all local authorities and Becta and therefore is used across London as a standard. All policies can be personalised to you your school by adding in your school logo and adding highlighted information. The signing of the acceptable use policy will be for all schools and forms part of a legally binding contract and clearly sets out responsibilities.

Temporary staff will need to sign a simple statement form highlighting that they are aware of data security and should ask if they have any concerns about working with data. Other adults working with children in a paid or voluntary capacity will also need to sign a form; this will include agency staff. Model forms are available.

You will need to make sure that acceptable use policies are signed by administrative workers.

Members of staff working remotely will need to sign a separate policy.