**Foxfield School**



**E-Data storage Policy**

**Updated November 2018**

**Senior Member of Staff Responsible:** Mr Paul Howley

**Designated Member of Staff:** Mr Steve Ledson

**Governor Responsible:** Councillor Mr Steve Williams

Contents

* General Data storage information and regulation
* Security procedures
* Disposal of equipment and e-data
* Storing and transfer of e-data
* Safe use of images and video
* Storage of images and video
* CCTV

**Data accuracy**

Data held will be as accurate and up to date as is reasonably possible. If a data subject informs the School of a change of circumstances their computer record will be updated as soon as is practicable. A printout of their data record will be provided to data subjects every twelve months so they can check its accuracy and make any amendments. Where a data subject challenges the accuracy of their data, the School will immediately mark the record as potentially inaccurate, or 'challenged'. In the case of any dispute, we shall try to resolve the issue informally, but if this proves impossible, disputes will be referred to the Governing Body for their judgement. If the problem cannot be resolved at this stage, either side may seek independent arbitration. Until resolved the 'challenged' marker will remain and all disclosures of the affected information will contain both versions of the information.

**Data adequacy and relevance**

Data held about people will be adequate, relevant and not excessive in relation to the purpose for which the data is being held. In order to ensure compliance with this principle, the School will check records regularly for missing, irrelevant or seemingly excessive information and may contact data subjects to verify certain items of data.

**Length of time**

Data held about individuals will not be kept for longer than necessary for the purposes registered, the length of time will be determined by the Records Management Society of Great Britain Local Government Group Retention Guidelines for Schools (as amended). It is the duty of the Data Protection nominated officer to ensure that obsolete data are properly erased.

**Data and computer security**

Foxfield School undertakes to ensure security of personal data by the following general methods (precise details cannot, of course, be revealed)

1. **Physical security**

Appropriate building security measures are in place, such as alarms, window bars, deadlocks and computer hardware cable locks. Only authorised persons are allowed in the computer room. Disks, tapes and printouts are locked away securely when not in use.

Visitors to the school are required to sign in and out, to wear identification badges whilst in the school and are, where appropriate, accompanied.

1. **Logical security**

Security software is installed on all computers containing personal data. Only authorised users are allowed access to the computer files and password changes are regularly undertaken. Computer files are backed up (i.e. security copies are taken) regularly.

1. **Procedural security**

In order to be given authorised access to the computer, staff will have to undergo checks and will sign a confidentiality agreement. All staff are trained in their Data Protection obligations and their knowledge updated as necessary. Computer printouts as well as source documents are shredded before disposal.

Overall security policy for data is determined by The Governing Body and is monitored and reviewed regularly, especially if a security loophole or breach becomes apparent. The School's security policy is available to staff.

Any queries or concerns about security of data in the school should in the first instance be referred to The Head teacher. Individual members of staff can be personally liable in law under the terms of the Data Protection Acts. They may also be subject to claims for damages from persons who believe that they have been harmed as a result of inaccuracy, unauthorised use or disclosure of their data. A deliberate breach of this Data Protection Policy will be treated as disciplinary matter, and serious breaches could lead to dismissal

**Security**

* The School gives relevant staff access to its Management Information System, with a unique ID and password
* It is the responsibility of everyone to keep passwords secure
* Staff are aware of their responsibility when accessing school data
* Staff have been issued with the relevant guidance documents and the Policy for Computing Acceptable Use
* Staff have read the relevant guidance documents available on the EGfL website
* Leadership have identified Senior Information Risk Owner (SIRO) and Asset Information Owner(s) (AIO)
* Staff keep all school related data secure. This includes all personal, sensitive, confidential or classified data
* Staff should avoid leaving any portable or mobile Computing equipment or removable storage media in unattended vehicles. Where this is not possible, keep it locked out of sight
* Staff should always carry portable and mobile Computing equipment or removable media as hand luggage, and keep it under your control at all times
* It is the responsibility of individual staff to ensure the security of any personal, sensitive, confidential and classified information contained in documents faxed, copied, scanned or printed.

This is particularly important when shared copiers (multi-function print, fax, scan and copiers) are used. Anyone expecting a confidential/sensitive fax, should have warned the sender to notify before it is sent using the Safe Haven Fax procedure below:

**Safe Haven Fax procedures**

When sending personally identifiable information:

* ensure the recipient knows the fax is being sent.
* ensure the fax will be collected at the other end.
* send the front sheet through first
* check that it has been received by the correct recipient.
* add the rest of the document to the fax.
* press the redial button.
* don’t walk away while transmitting.
* wait for the original to process and remove it from the fax machine.
* wait for confirmation of successful transmission.
* confirm whether it is appropriate to fax to another colleague if they are not there to receive it.
* use only the minimum information and anonymise where possible

**Disposal of Redundant Computing Equipment Policy**

* All redundant Computing equipment that may have held personal data will have the storage media over written multiple times to ensure the data is irretrievably destroyed. Or if the storage media has failed it will be physically destroyed.
* The school will maintain a comprehensive inventory of all its Computing equipment including a record of disposal
* The school’s disposal record will include:
  + Date item disposed of
  + Authorisation for disposal, including:
    - verification of software licensing
    - any personal data likely to be held on the storage media? \*
* How it was disposed of e.g. waste, gift, sale
* Name of person & / or organisation who received the disposed item\* if personal data is likely to be held the storage media will be over written multiple times to ensure the data is irretrievably destroyed.
* Any redundant Computing equipment being considered for sale / gift will have been subject to a recent electrical safety check and hold a valid PAT certificate

**Storing/Transferring Personal, Sensitive, Confidential or Classified Information Using Removable Media**

* Ensure removable media is purchased with encryption
* Store all removable media securely (e.g. cameras, ipads)
* Securely dispose of removable media that may hold personal data
* Encrypt all files containing personal, sensitive, confidential or classified data
* Ensure hard drives from machines no longer in service are removed and stored securely or wipe clean

This information will include (but not fully inclusive);

* Any Personal staff and pupil data
* Assessment data
* Images and videos
* Behaviour management information
* Annual reviews
* Annual reports

**Safe Use of Images**

Taking of Images and Film Digital images are easy to capture, reproduce and publish and, therefore, misuse. We must remember that it is not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness. ECC guidance can be

found: <http://esi.essexcc.gov.uk/vip8/si/esi/content/binaries/documents/Service_Areas/Governance/Information_Governance_doc_February_2010_2.doc>

* With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment
* Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, this includes when on field trips. However with the express permission of the Headteacher, images can be taken provided they are transferred immediately and solely to the schools’ network and deleted from the staff device

**Consent of Adults Who Work at the School**

* Permission to use images of all staff who work at the school is sought on induction and a copy is located in the personnel file

Publishing Pupil’s Images and Work On a child’s entry to the school, all parents/carers will be asked to give permission to use their child's work/photos in the following ways:

* on the school web site
* on the school’s Learning Platform
* in the school prospectus and other printed publications that the school may produce for promotional purposes
* recorded/ transmitted on a video or webcam
* in display material that may be used in the school’s communal area
* in display material that may be used in external areas, i.e. exhibition promoting the school
* general media appearances, e.g. local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically)

This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child’s circumstances where consent could be an issue, e.g. divorce of parents, custody issues, etc.

Parents/ carers may withdraw permission, in writing, at any time. Consent has to be given by both parents in order for it to be deemed valid.

Pupils’ names will not be published alongside their image and vice versa. E-mail and postal addresses of pupils will not be published. Pupils’ full names will not be published. Before posting student work on the Internet, a check needs to be made to ensure that permission has been given for work to be displayed.

Only the Web Site Manager (Deputy Headteacher) can give authority to upload to the site.

**Storage of Images**

* Images/ films of children are stored on the schools media network
* Pupils and staff are not permitted to use personal portable media for storage of images (e.g., USB sticks) without the express permission of the Headteacher
* Rights of access to this material are restricted to the teaching staff and pupils within the confines of the school network/ Learning Platform

Images should be removed from mobile devices Cameras, ipads at the earliest possible opportunity

* All devises to be encrypted or pass-coded where possible

**Webcams and CCTV**

* The school uses CCTV for security and safety. The only people with access to this are SLT and designated staff. Notification of CCTV use is displayed at the front of the school. We do not use publicly accessible webcams in school
* Webcams in school are only ever used for specific learning purposes, i.e. monitoring hens ‟eggs, school show (used secured link), assessment (secured) and education
* Misuse of the webcam by any member of the school community will result in sanctions (as listed under the *see Paul*)
* Consent is sought from parents/carers and staff on joining the school, in the same way as for all images