PRIOR HEATH INFANT SCHOOL
POLICY AND PROCEDURES STATEMENT

TITLE: Data Protection and Handling Policy **DATE: November 2017**
REVIEW: as necessary

APPROVED/MONITORED BY: Resource Committee
AGREED BY: WHOLE SCHOOL STAFF and GOVERNORS

Prior Heath is aware of its duties and obligations under the Data Protection Legislation 1998 and is registered as a data controller with the Information Commissioner's Office.

The Head Teacher supported by the named DP Officer (the Bursar) has overall responsibility for Data Protection and Handling within the school. Staff are responsible for their safe handling of potentially sensitive data and adopt good information handling principles to present claims, fines or bad publicity or damage to the reputation of the school or staff as follows:-.

- Fairly and lawfully processed, including issuing of Pupil and Employee privacy notices
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate and up to date
- Kept no longer than necessary
- Processed in line with individual's rights
- Kept securely
- Destroyed securely
- Shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

<u>Requests will only be actioned from:</u>

Parents or those with parental responsibility

- in own right as parent (educational records see below)
- on behalf of child where consent given from child who is competent to understand
- child if competent as above
- Solicitors acting for parent/child – need consent from parent/child as appropriate
- from police, having checked identification, when submitted in writing and signed by a senior officer. Minimum required for them to be able to prevent or detect a crime or apprehend or prosecute an offender without consent from individual, however, if there are genuine concerns, such as the

information is confidential, we may ask the police to come back with a court order. Advice will be sought from Legal Services or LEO
- the LA, DfE and between schools via secure file transfer
- Employees for their own personal data

Requests will be fulfilled in one of the following ways:

- Hard copy with careful check on redaction
- Electronic after converting to pdf
- Send direct to recipient and not through 3rd party wherever possible (ie Solicitor)
- An employee may check through their own file in the presence of the Head Teacher or Bursar

Education Records – we will not disclose the following information:

- That regards child protection, where the disclosure would not be in the best interests of the child
- That is likely to cause serious harm to the physical or mental health or condition of the child or someone else
- References supplied to potential employers of the child (keep factual and relevant as employer may be asked to disclose)
- Some court reports
- Information recorded by the pupil during an examination
- Third party personal information without consent unless reasonable in all circumstances
- Legal advice given to the school

Timescales for requests:

- Disclosure of pupils manual and computerised records within 15 days of request in writing
- An employee's personal file with be disclosed, once confidential references supplied by third parties and any other third party information is removed, within 24 hours during term time, of request in writing to the head teacher
- If a hard copy of record is requested as per our Freedom of Information Act Publication Scheme a charge will be made.

Risks have been identified and the following arrangements are in place to prevent Data Protection breaches:

- Staff and parents all receive a copy of the relevant privacy notice.
- All staff must log of from sensitive drives when leaving their work stations
- Staff must carefully check the intended recipient before sending all emails

- Staff must carefully check photocopying before dispatch to ensure there is no inclusion of pages not intended for recipient and that they reach the correct recipient
- Where appropriate, password protected queuing from classroom and office computers to photocopier are in place
- Sufficient password control for pcs and laptop – under the Staff Acceptable Use/Code of Conduct for ICT Policy passwords must be changed frequently and not disclosed to anyone other than an authorised system manager
- Encrypted devices only used where Ranger remote access unavailable. (Encrypted memory sticks to be borrowed from office) No personal information to be kept on any device except school server. (See Staff Acceptable Use/Code of Conduct for ICT Policy)
- Where Ranger remote access has been used files must be removed once data has been transferred back to the server. All personal PCs/laptops must have up to date antivirus software and malware.
- Remote backup/restore of all school data is managed by Babcock 4S. No tapes are stored on site.
- All cloud based storage systems (ie RM Easymail and Redstone remote backup storage facilities) are Surrey recommended systems.
- Data Protection clauses will be included in any contract where data is likely to be passed to a third party.
- No personnel files to be taken off site
- No children's files to be taken off site
- Staff directed not to discuss personal information outside of school or within school where parents may be around
- Paper SEN, Personnel and Children's records are kept in locked cabinets
- Shredding of paperwork containing personal/confidential information in place.
- Any company used to shred material must do so on site and provide certificates to indicate this has taken place.
- Hard drives from devices are disposed of according to legal requirements. Data Destruction Certificates are required by us for all IT equipment being recycled or destroyed. These records are maintained by the Bursar.
- Information will not be placed on social media sites.
- Training is carried out annually to keep staff up to date with best practice.
- This policy is circulated to all staff to remind them of their responsibilities.
- This policy is included in the Staff Handbook.

<u>Data Breaches – accidental or deliberate loss of data or breaches of Data Protections and Data Handling or Staff Acceptable/Code of Conduct for ICT policies:</u>

- A log will be kept by the Bursar of any breaches.
- All breaches must be reported to the Head Teacher as soon as they occur.
- The Head Teacher and the Data Protection Officer are responsible for establishing a plan of action, including escalation procedures to produce a rapid resolution.

- The Head Teacher and the Data Protection Officer are responsible for taking any necessary actions to prevent recurrence and establish awareness training.
- All significant incidents will be reported via the SIRO to the Information Commission Office.
- Advice will be taken where necessary from Legal Services and the Local Education Office.

Other information:
A record of all requests for freedom of information requests will kept by the Bursar.