Brady Primary School

Data Protection Policy

'All children can learn considerably more'

Aims of Brady Primary School

"All children can learn considerably more"

At Brady Primary School we aim to provide a safe, caring and stimulating environment, which offers opportunities:-

- For everyone within the school to reach their full potential and develop self-worth, self-confidence, the ability to take responsibility for their own individual actions, and resilience.
- For everyone within the school to have a sense of wonder, an enthusiasm for learning and help children to develop as independent thinkers and learners with enquiring minds.
- To encourage and develop a respect and understanding for others.
- To develop all partnerships, small and large, from the individual parent to the wider community and beyond to support children's learning.
- To give children access to a broad and balanced creative curriculum to attain the highest possible standards in relation to prior attainment through assessment, teaching and learning.

Equal opportunities and Inclusion

At Brady Primary school we believe that every child is entitled to equal access to the curriculum, regardless of race, gender, class or disability.

We are committed to promoting learning and teaching environments, for all that embed the values of inclusive educational practices.

Through a child centred approach, we aim to ensure that education is accessible and relevant to all our learners, to respect each other and to celebrate diversity and difference.

Strategic and operational practices:

At this school:

- The Head Teacher is the Senior Information Risk Officer (SIRO).
- Staff are clear who the key contact(s) for key school information are (the Information Asset Owners). We have listed the information and information asset owners in a spreadsheet.
- We ensure staff know to immediately report, and who to report to, any incidents where data protection may have been compromised, such as when passwords for sensitive systems or devices are lost or stolen, so that relevant action(s) can be taken.
- All staff are DBS checked and records are held in one central record SIMS.

  We ensure ALL the following school stakeholders sign an Acceptable Use Agreement form. We have a system so we know who has signed.

  - staff
  - governors
  - pupils
  - parents
  - volunteers

  This makes clear all responsibilities and expectations with regard to data security.
- We have approved educational web filtering across our wired and wireless networks.
- We follow LA guidelines for the transfer of any data, such as MIS data or reports of children, to professionals working in the Local Authority or their partners in Children's Services / Family Services, Health, Welfare and Social Services.
- All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their passwords private.
- We require staff to use STRONG passwords for access into our MIS system.
- We require staff to change their passwords into the MIS, USO admin site, every 90 days or once a term.
- School staff who set up usernames and passwords for e-mail, network access are working within the approved system and follow the security processes required by those systems.

- We ask staff to undertake house-keeping checks at least annually to review, remove and destroy any digital materials and documents which need no longer be stored.

Technical or manual solutions:

- Staff have secure area(s) on the network to store sensitive documents or photographs.
- We require staff to log-out of systems when leaving their computer, but also enforce lock-out after 10 mins. idle time.
- We use the DfE S2S site to securely transfer CTF pupil data files to DfE / other schools.
- We use the Pan-London Admissions system to transfer admissions data.

- We use LGfL AutoUpdate for creation of online user accounts for access to broadband services.
- We store any Protect and Restricted written material in a lockable storage area.
- All servers are in lockable locations and managed by DBS-checked staff.
- We use Joskos' remote secure back-up for disaster recovery on our network /admin/ curriculum servers.
- We comply with the WEEE directive on equipment disposal, by using an approved disposal company for disposal of IT equipment. For systems, where any protected or restricted data has been held, (such as servers, photocopiers), we get a certificate of secure deletion.
- Portable equipment loaned by the school (for use by staff at home), where used for any protected data, is disposed of through the same procedure.
- Paper based sensitive information is shredded, using a cross-cut shredder or disposed of by using Lyreco's confidential shredding service.

Review

This policy will be reviewed at least every two years by the Leadership and Management Committee. Any alterations that come from this review will be discussed with the Headteacher and ratified by the teaching staff and appropriate governing body sub-committee.

Chair of Governors …… Date ……..

Headteacher …… Date ……..