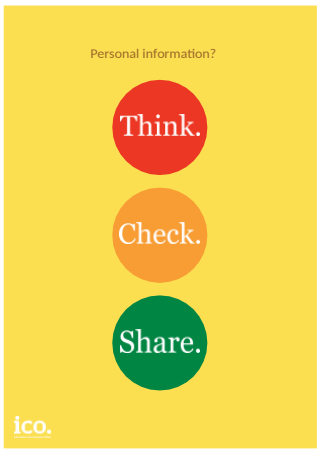
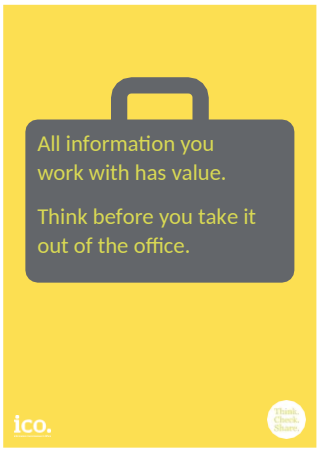
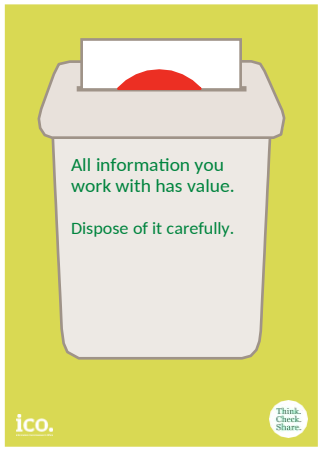
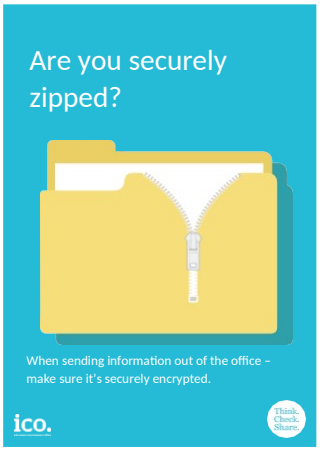
Brady Primary School –GDPR handbook for Staff (including Staff Privacy Notice)

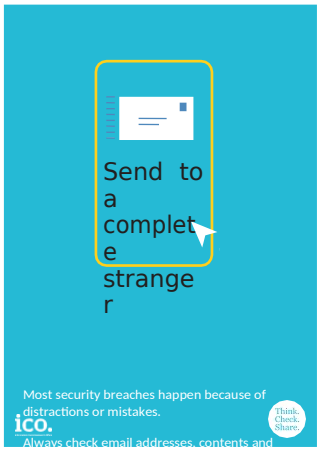
Communicating the importance of information security to staff

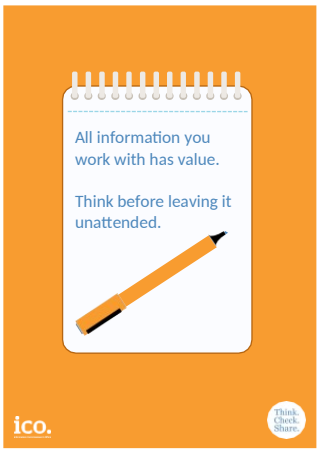


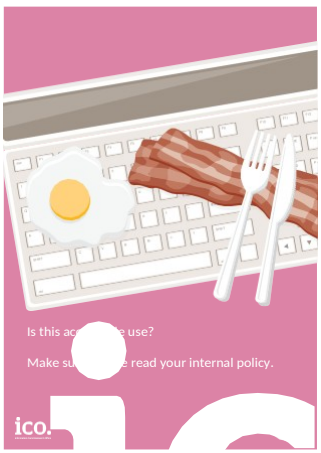


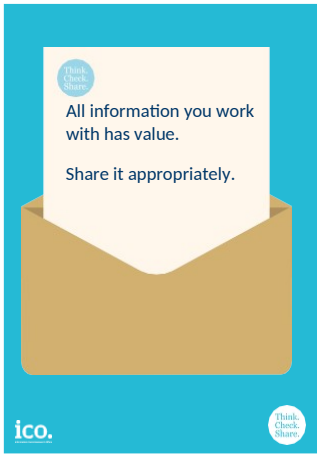


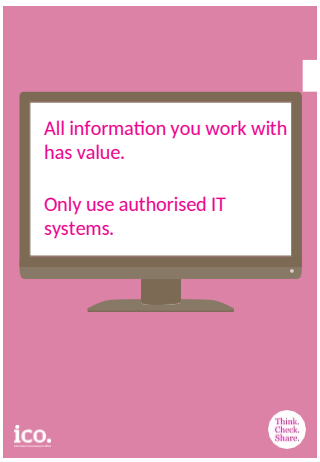












Tips for Teachers and Support Staff to Protect Data

1. Lock your computer when logged on if you have to leave it unattended. (ctrl,alt,del - select lock)
2. **DO NOT GIVE YOUR USER NAME AND PASSWORD TO ANYONE**.
3. Please log out of your computer at the end of the day. If a user is logged in please logout before using the device.
4. Do not save your password in the Web Browser.
5. Make sure you log out of your mail/drive/ etc – do not just close the window.
6. Do not leave personal or sensitive information unattended. Lock it away in lockable drawers Make sure you do not have personal or sensitive data shown on the whiteboard e.g. sims/assessment/planning/reports.
7. Only use a school email address for work related emails. Check address carefully before pressing send.
8. Do not send personal or sensitive information via email to a third party unless checked with the office.
9. **No memory sticks to be used**.
10. Your home computer should have up to date virus software if you are using it to access personal or sensitive information
11. Working at home should be through the RDS software. Data to be deleted from your device once uploaded.
12. If you have a visitor presenting or using the Wi-Fi – they will need to sign an Acceptable Use Policy.
13. If you download personal or sensitive information on a personal device, you must upload back to drive and delete. You must not leave on your local machine.
14. You must have a pin number on your mobile device if you have school email on it.

Paper

15. Keep all paper containing personal or sensitive information safe, secure and away from others e.g. not on the desk/ or on display.
16. Do not leave personal or sensitive data by the printer.
17. **DO NOT LET PUPILS BRING CONFIDENTIAL DOCUMENTS OR WASTE TO THE OFFICE**
18. Dispose of paper that contains personal or sensitive information in the Data sack which will be in the office. **NEVER throw it away in the bin** (this includes post it notes).
19. Check first with the Data Compliance Team (MN/ SS) before signing up to third party solutions for processing and storing personal or sensitive data that consent is not required from learners and/or parents before it can be used e.g. Curriculum Subscriptions like Timestable Rockstars.
20. If you have a list of children displayed only use first names i.e. Milk lists/medical etc

General

21. Never speak to a parent regarding a child outside in the playground take them to a private area.
22. Be aware of who is around if you are making phone calls to parents – do not phone from office if children are in office.
23. Never take photos on your personal devices.
24. If you want to take personal or sensitive information offsite it must be authorised and logged in/out via the office e.g Trip lists with mobile phones numbers.
25. Medication taken on trips etc, must be logged out and back in.

What is Personal and Sensitive Data?

All Information held electronically or in structured files that tells you something about an identifiable living individual. This would extend to all information in education records – examples of this:

Personal Data - Children and Staff

1. Full Names
2. Address
3. Date of Birth
4. School
5. Exam results information
6. Medical Information
7. National Insurance Number
8. Staff Development and reviews
9. SEN Assessments and Data
10. Photos

Sensitive Data - Children and Staff

1. Race and Ethnicity
2. Political Opinions
3. Religious Beliefs
4. Membership of Trade Union
5. Physical or Mental Health
6. Sexuality
7. Criminal offences

What are Key Subject's Rights?

- the right to be informed
- the right of access
- the right to rectification
- the right to erasure
- the right to restrict processing
- the right to data portability
- the right to object
- rights in relation to automated decision making and profiling

It means the data subject (parents & staff) receives clear communications about:

- what information is being collected/processed about them (in detail)
- why the data is collected (purpose)
- what the lawful basis for collecting and holding the data is (where applicable)
- who/which organisations data is shared with and why
- how the data is stored and how long for, and how security is ensured
- how to exercise their right of access to data
- how to exercise any other rights, such as restricting certain types of processing (for example biometric data) or to rectify data
- who to contact for queries

At Brady Primary we communicate this via Privacy notices and the website.

Subject Access Requests (SARs)

Access to personal data held by the school used to be something that had to be applied for – and paid for. It now has to be provided for free and within a very tight time scale.

SARs include ALL information held about a subject – including emails, notes etc. For this reason, it is recommended that important notes from email transcripts are copied down and then emails deleted to enable swifter access to information should it be requested.

Staff are reminded to use professional language only in emails to parents – and to colleagues regarding pupil matters – as these emails could be requested in a SAR!

Data Breaches

Where data is inadvertently lost, displayed or given to the wrong person, it is important to report this either in person to the Compliance team and on-line on the GDPRis website.

Most cases will be easily resolved but, in some cases, this might need to be reported to the Data Protection Officer (DPO) Tracey Walker- dpo@brady.havering.sch.uk, who might refer it on to the Information Commission Officer.

Parents and staff have the right to refer breaches directly to the DPO.

The important thing to remember is to be vigilant, think before sharing any data and be particularly careful with paperwork.

Below are some examples of breach scenarios;

- the safeguarding lead was emailing two MARFs (multi agency referral forms) to a colleague in Mental Health services. After pressing send they realized they had sent them to a midday assistant by mistake;
- a member of the public phones the school office to say your school website has a list of pupils who are in the football team, and details of the fixtures this term;
- a staff member walks to work; it was a nice morning, they stopped in the park and have left their laptop on a bench- it isn't there now.
- it's parents evening, you are walking round the school when you see a teacher has projected on the whiteboard, in their classroom, a class list with progress and attainment data for maths;
- a colleague had an email from the LA about 2 children detailing issues the person was to take up with the families; the original email was forwarded on to 2 sets of parents and one of the parents has phoned the school to complain.

Personal Data Breach Procedures

This procedure is based on guidance on personal data breaches produced by the ICO.

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the school's Data compliance team (DCT) Michael Nunn and Sharon Smith and report this on GDPRiS
- The Data compliance team will investigate the report and determine whether a breach has occurred and whether this needs to be reported to the Data Protection Officer (DPO). To decide, they will consider whether personal data has been accidentally or unlawfully:
    - Lost
    - Stolen
    - Destroyed
    - Altered
    - Disclosed or made available where it should not have been
    - Made available to unauthorised people.
- The DCT/DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary.
- The DCT/DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen
- The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
    - Loss of control over their data
    - Discrimination
    - Identify theft or fraud
    - Financial loss
    - Unauthorised reversal of pseudonymisation (for example, key-coding)
    - Damage to reputation
    - Loss of confidentiality
    - Any other significant economic or social disadvantage to the individual(s) concerned.

  If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.
- The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored on GDPRis and in a folder in HT room.
- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the DPO will set out:
    - A description of the nature of the personal data breach including, where possible:
        - the categories and approximate number of individuals concerned
        - the categories and approximate number of personal data records concerned
    - The name and contact details of the DPO

    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned.
- If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible
- The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned.
- The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
    - Facts and cause
    - Effects
    - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

  Records of all breaches will be stored on GDPRis
- The DCT/DPO and Headteacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible.

Actions to minimize the impact of data breaches

We will take actions to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

Brady Primary School's GDPR privacy notice for the school workforce

Schools are currently required to detail to staff how their personal data may be collected and used. This requirement will remain once the General Data Protection Regulation (GDPR) comes into effect on 25 May 2018; however, schools will be required to revise their privacy notices to include further information on processing individuals' personal data. Schools can use this template privacy notice to ensure they are compliant with the GDPR and communicate how they process personal data relating to the school workforce.

The school workforce

Who processes your information?

The school is the data controller of the personal information you provide to us. This means they determine the purposes for which, and the manner in which, any personal data relating to staff is to be processed. A representative of the school, Michael Nunn, can be contacted on 01708 555025 or office@brady.havering.sch.uk.

Tracey Walker is the data protection officer. Their role is to oversee and monitor the school's data processing practices. This individual can be contacted on dpo@brady.havering.sch.uk

Where necessary, third parties may be responsible for processing staff members' personal information. Where this is required, the school places data protection requirements on third party processors to ensure data is processed in line staff members' privacy rights.

Why do we need your information?

Brady Primary School has the legal right and a legitimate interest to collect and process personal data relating to those we employ to work at the school, or those otherwise contracted to work at the school. We process personal data in order to meet the safeguarding requirements set out in UK employment and childcare law, including those in relation to the following:

- Schools Funding Agreement
- School's legal framework
- Safeguarding Vulnerable Groups Act 2006
- The Childcare (Disqualification) Regulations 2009

Staff members' personal data is also processed to assist in the running of the school, and to enable individuals to be paid.

If staff members fail to provide their personal data, there may be significant consequences. This includes the following:

- Employment checks:

- Failure to provide the school with ample proof of a right to work in the UK will prevent employment at name of school.
- Employees found to be working illegally could face prosecution by law enforcement officers.
- Salary requirements:
- Failure to provide accurate tax codes and/or national insurance numbers could lead to issues of delayed payments or an employee paying too much tax.

For which purposes are your personal data processed?

In accordance with the above, staff members' personal data is used for the following reasons:

- Contractual requirements
- Employment checks, e.g. right to work in the UK
- Salary requirements
- DBS checks
- Unemployment Benefit Department - information if required

Which data is collected?

The personal data the school will collect from the school workforce includes the following:

- Names
- National insurance numbers
- Characteristics such as ethnic group
- Employment contracts
- Remuneration details
- Qualifications
- Absence information
- Teachers DFE number

The collection of personal information will benefit both the DfE and LA by:

- Improving the management of workforce data across the sector.
- Enabling the development of a comprehensive picture of the workforce and how it is deployed.
- Informing the development of recruitment and retention policies.
- Allowing better financial modelling and planning.
- Enabling ethnicity and disability monitoring.
- Supporting the work of the school teachers' review body.

Will your personal data be sought from third parties?

Staff members' personal data is only sought from the data subject. No third parties will be contacted to obtain staff members' personal data without the data subject's consent.

Staff members' personal data may be obtained and processed from third parties where the law requires the school to do so, e.g. medical records from a GP. The categories of data obtained and processed from third parties include:

Where data is obtained from third parties, the personal data originates from the following sources:

How is your information shared?

Brady Primary School will not share your personal information with any third parties without your consent, unless the law allows us to do so.

We are required, by law, to pass on some personal information to our LA and the DfE. This includes the following:

How long is your data retained for?

Staff members' personal data is retained in line with Brady Primary School's Records Management Policy.

Personal information may be retained for the following periods depending on the nature of the information. Data will only be retained for as long as is necessary to fulfil the purposes for which it was processed, and will not be retained indefinitely.

If you require further information regarding retention of data, and the periods for which your personal data is held for, please download our **Records Management Policy**. This in in line with Annex 5.1 of DFE's Data protection: a toolkit for schools.

What are your rights?

As the data subject, you have specific rights to the processing of your data.

You have a legal right to:

- Request access to the personal data that Brady Primary School holds. Subject Access Request- **please be aware that the school does not receive and read emails and letters during school holiday periods.**
- Request that your personal data is amended.
- Request that your personal data is erased.
- Request that the processing of your data is restricted.

Where the processing of your data is based on your explicit consent, you have the right to withdraw this consent at any time. This will not affect any personal data that has been processed prior to withdrawing consent.

Staff members also have the right to lodge a complaint with the Information Commissioner's Office (ICO) in relation to how Brady Primary School processes their personal data.

How can you find out more information?

If you require further information about how we and/or the DfE store and use your personal data, please visit our website, **http://www.bradyprimaryschool.co.uk** the Gov.UK website, or download our **GDPR Data Protection Policy** and **Records Management Policy**.

Explaining the Language around data protection

Term	Description	Example
Data subject	The person that the data relates to.	John Smith the pupil. Jane Smith the teacher.
Data item	A single piece of information about a data subject.	"Ethnicity = white British" "Attendance = 97%"
Data item group	A group of data items that are typically captured about the same activity or business process in school. These are also sometimes called data elements or data scope within the data community/sharing agreements schools have with suppliers.	Behaviour management, or catering.
System	A piece of software, computer package or manually managed asset that supports the administration of one or more areas of school life.	Capita SIMS, ParentPay
System group	An umbrella term to describe the areas of school administration where systems that contain personal level data typically reside.	Core MIS, payments, curriculum tools.
Personal data	Information relating to a natural identifiable person, whether directly or indirectly	John Smith was born on 01/01/1990. The head teacher's salary is £60,000.
	These are highly sensitive pieces of information about people. They are important because under GDPR they are afforded extra protection in terms of the reasons you need to have to access and process that information. In education, it would also be best practice to treat things	Tightly defined as data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, health, trade-union membership, and health or sex life. Data relating to criminal offences is also afforded similar special protection.

	like FSM, SEN, and CIN/CLA status as special category data.	
Term	**Description**	**Example**
(Data) Controller	The organisation who (either alone or in common with other people) determine the purpose for which, and the manner in which data are processed.	A school is often the data controller, sometimes a joint controller with the LA or DfE.
(Data) Processor	A person or organisation who process data on behalf of and on the orders of a controller.	A catering supplier the school uses.
Data audit/data asset register	The assessment of data and its quality, for a specific purpose. Other terms you might hear are data map or information asset log. In this context, we simply want the list of personal data assets that we hold, from which we can go on to place further important information alongside.	
Lawful basis and conditions for processing	These are the specific reasons, set out in law, for which you can process personal data. There is one list for personal data (lawful basis article 6) and another list for processing special category data (article 9).	"The processing is necessary for administering justice, or for exercising statutory or governmental functions." Read the full list.
Data retention	How long you will hold information for to do the processing job you need it for. At the end of a data retention period, processes should be in place to ensure it is properly disposed of.	"We keep parent's phone numbers until 1 month after they leave the school in case of any issues that need resolving (for example, payment or repayment of lunch money) and then it is deleted."
Privacy notice	This is a document that explains to the people you have data about ("data subjects") the data items you hold, what they are used for, who it is passed onto and why, and what rights they have.	DfE publish model privacy notices.

Term	Description	Example
Subject Access Request (SAR)	This is where a person (data subject), requests access to the information you hold about them. Timescales for responding, as well as reasons why you must comply or may refuse, as set out in law. A Subject Access Request is often used to describe “tell me all my data you hold”.	“I want to know the attendance data you hold about my son”
Data Protection Impact Assessment (DPIA)	This is a process to consider the implications of some change you are introducing on the privacy of individuals. Assessing privacy at the outset helps you plan consultation/awareness/consent type options from the outset. “Privacy by design” is a term that is used in this space.	You would undertake one of these if introducing a new system to use fingerprinting within catering provision.
Data breach	A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.	Sending a list of pupil names, attainment marks and dates of births to the wrong school.
Automated decision making/profiling	This is when machines/software apply rules to data and determine something about someone based on purely applying those rules. Typically it is the significance of the decision which drives the caution and concern here. Read further information.	“Anyone recorded as attendance >99% will get a voucher for X”