Brookfield Primary School Policies – GDPR Policy for School Staff

Brookfield Primary School

Record of Policy Amendment / History

Date Approved	Minute No.
07/10/2021	2094.21

Brookfield Primary School

'Be the best you can be'

GDPR POLICY FOR SCHOOL STAFF

Brookfield Primary School aims to provide an educational environment of the highest quality in which we will strive to:

- To keep every pupil safe
- Develop effective and enthusiastic learners
- Value the self esteem and maximise the potential of every child
- Promote constructive attitudes and values
- Foster caring relationships in a secure environment
- Work in equal partnership with parents and carers and involve them in their children's learning

STAFF CODE OF CONDUCT

It is the responsibility of the School's Senior Leadership Team in association with the School's nominated DPO to ensure that all employees have appropriate training in information security and confidentiality.

Brookfield Primary School is clear about what we expect of our employees in relation to information and confidentiality. You may have access to restricted, controlled or confidential information in the course of our work. You must protect that information in accordance with the policies of procedures of our school and you must not disclose that information or use that information for your own purposes, benefit or gain, or to discredit the school, or pass information to toehrs who may use it in such a way.

As an employee you must be aware of your responsibility for secure personal and confidential information hadnling and mangement. This might include;

- Paper records
- Mail both internal and external
- Verbal communications
- Electronic records
- Establishment security
- Taking work outside the workplace
- Information sharing
- Management of confidential information and how this is passed on
- The potential for breaches of security or confidentiality

CONTENT

This policy will provide YOU with guidance about;

- Information Governance
- Caldicott Principles
- Data Protection and the new Genernal Data Protection Regulation (GDPR) May 2018
- Confidentiality
- Freedom of Informatin
- Records Mangement

This will also enable you to reduce the risk to security and to data breaches. Everybody in school is repsonsible for the security of data even if it is in a small way.

INTRODUCTION

General Data Protetion Regulation, known as "GDPR" and the Data Protection Act 2018 came into effect on 25th May 2018. Some of the changes to current Data Protection practise are included to ensure Brookfield Primary School remains compliant.

Brookfield Primary School takes its responsibility for data security very seriously. Any breach of the Data Protection Act can lead to large fines, money that the school could better utilised for the Education of its pupils. An example of data breach is loss of papers that might contain student, staff or contact information. Such an incident should be reported immediately to the Headteacher, a member of the Senior Leadership Team or your school's nominated Data Protection Officer; HT/SLT/DPO.

An employee responsible for a breach of the rules could face disciplinary aciton or possibly a fine from the Information Comminssioners Office. It is in your own interest to look after any information (data) you have. Data privacy is relevant to everyone and every one's responsbility.

INFORMATION GOVERNANCE

Information Governance is the framework which enables the organisation; the school and you as an employee to comply with legal and statutory requirements.

Underpinning the Information Governance Framework, in regard to personal data, is the General Data Protection Regulation and the Data Protection Act 2018,

THE DATA PROTECTION ACT

Under the new General Data Protection Regulation (GDPR) and the new Data Protection Act 2018, there are **six Privacy Principles** that all schools must comply with;

1. **Lawfulness, fairness and transparancy**
   The first principle in the regulation is all about handling your client's personal data* in a fair and honest way. Pupils, contacts or staff are all clients. It should be explained what type of data you collect, why you collet it and how you plan to use it.

2. **Purpose Limitations**
   The second principle talks about only using someone's personal data for the resasons that they have agreed to.

3. **Data minimisation**
   The thrid principle is similar to the second and talks about only gathering the data that you really need in order to carry out the services provided.

4. **Accuracy**
   The fourth pricniple is very straightforward. Data must be accurate. If its not accurate you must try to update it.

*Data can be electronic or paper based.

5. **Storage limitations**
   The fifth principle talks about only storing personal data for as long as we need it and deleting it after that point. Guidance on this can be found in the School's Retention Policy or Schedule.

6. **Integrity and confidentiality**
   The sixth principle is all about the security of the personal data that we hold. Security is more that just getting hacked, it covers loss and unauthorised use of data as well. Technical security is important, for example, making sure that only authorised people have access to the data and strong passwords used. Brookfield Primary School have taken mesures e.g. using only encrypted memory sticks to save confidential items onto, to ensure only authorised people have access to the data stored.

UNIVERSAL PRINCIPLES FOR USING PERSONAL DATA AKA 'THE CALDICOTT PRINCIPLES'

As well as the '6 Privacy Principles', there are **7 Universal Principles for using Personal Data.** Simply put, these are the principles we will adhere to when using personal data and are widely known as the 'Caldicot Key Principles'.

Where information under consideration includes client information, the Caldicott principles apply. Pupils/studens, contacts or staff are all clients. These are listed as follows;

1. **Justify** the purpose

2. Don't use personal identifable information unless it is **absolutely necessary**

3. Use the **minimum necessary** personal-identifiable information

4. Access to personal identifiable information should be on a **strict need-to-know** basis

5. Everyone with access to person identifiable information should **be aware of their responsibilities**

6. Understand and **comply with the law**

7. **The duty to share information can be as important as the duty to proect service user confidentiality** e.g. for stafeguarding reasons

Whilst keeping data safe is very important it cannot stand in the way of those tasks which are essential to safeguard, educate and ensure the wellbeing of the pupils we care for. These principles should not be to the detriment of carrying out everyday tasks.

For example, it is absolutely fine to apply children's names to their coatpegs ro aid name recognition and to help a child store its property.

Similarly it is reasonable for a teacher to retain a list of pupil names and academic achievement for the purpose of tracking progress whils in school. However, these records should always be kept safe.

PERSONAL DATA

Personal data is any information relating to an identified or identifable person aka 'the data subject'.

An identifiable person is one who can be identified, directly or indirectly, for example by name, location, appearance, identity number, social or economic context, online identifier genetic data etc. NOTE: In some cases more that one of these identifiers would be necessary to identiy an individual.

SUBJECT ACCESS REQUESTS

Anyone can ask to see what information the School hold on them, including any written notes and client logs.

The request can be made by the person themselve or someone with **authority** to represent them i.e. anyone with proven responsibility for the child e.g. parent or guardian but not necessarily any family member.

If you are made aware that the somebody is requesting a Subject Access Request you must advise someone from SLT or the School's DPO (Mrs Victoria Hardy DPO) immediately as the school must respond to these within **15 school days** of receiving it.

SAFEGUARDING AND THE DATA PROTECTION ACT

There may be tiems where you will need to share personal information where a person's safety or welfare is at risk. As long as you can justify your decision to share information under these circumstances and record it, you will not be in breach of the Act.

Safeguarding means the protection from maltreatment, preventing impairment to health or development, providing an environment of safe and effective care and promoting the best outcomes for children and vulnerable adults. If in doubt, speak to the school's Safeguarding Lead (Mrs Lynne Greenhough).

THE INFORMATION COMMISSIONER'S OFFICE; THE ICO

The ICO's mission is to uphold information rights in the public interest, promiting openess by public bodies and data privacy for individuals.

The ICO can prosecute those who commit criminal offences under the Act. Offences include;

- **Unlawfully obtaining or disclosing data or information**
- **Arranging the disclosure of personal data to someone else**
- **Selling personal data which was unlawfully obtained**

The ICO can

- **Issue monetary penalty notices, requiring organisations to pay out substantial amouts for serious breaches of the Data Protection Act**
  Fines can be issued to both organisations and the individuals who have broken one or more of the data protection principles. The fines can be considerable. Examples of serious Security Breaches can be explained in the next section.

- **Prosecute those who commit criminal offences under the Act**
- **Report to Parliament on data protection issues of concern**
- **Provide information and advice for individuals and organsiations**

More information can be found on the ICO's website; https://ico.org.uk

SECURITY BREACHES

Examples of security breaches include:

- Confidential information left on noticeboards that can be seen by the public through a door or window
- Client information left on car seats where it can be viewed by passers by
- Client information dropped on the street
- Discussions held in public; the street, corridors, other people's rooms etc where they can be overheard
- Loss of ID badges
- Confidential papers not disposed of correctly
- Uploading documents containing sensitive personal data
- Publising sensitive information about a family
- Discarding/leaving coduments containing personal details for one or many persons in a disused building
- Documents left in a carrier bag on a train or other method of public transport
- Documents containing sensitive information leftt in a second hand furniture sent to a shop for sale

Some of the above examples have received some sizeable fines from the ICO.

If you discover or commit an information security breach you should report it immediately to the HT/SLT/DPO. This will then be recorded on a n online incident report form.

CALLS AND CONVERSATIONS

- **Always** be aware of who can overhear confidential conversations
- **Never talk** about confidential work matters with friends, family and colleagues unless they need to know to do their job
- **Dont discuss** personal information relating to one client with another

INAPPROPRIATE USE OF INTERNET AND EMAIL

You are required to abide by Brookfield Primary School's Internet Acceptable Use Policy. The use of social media is also covered by this policy.

However, if you do accidently access inappropriate material on the web, inform the school HT/SLT/ or DPO. You may be asked to complete an Accidential Misuse of Email or Internet Form.

You must not download anything onto a work computer or open suspicious emails due to the risk of computer virus.

SOCIAL MEDIA AND CODE OF CONDUCT

All employees at Brookfield Primary School are expeted to behave appropriately and responsibly and should be aware that they may be accountable to the school for actions outside of their workplace.

Online conduct is the employee's responsibiltiy and it is important that employees are aware that posting information on social networking sties in a personal capactiy cannot be entirely isolated form their working life.

Any information published online can be accessed around the world within seconds and will be publicly available for all to see. It is not easy to delete/withdraw once published.

The school views any comment that is made on a socail media site as being in the public domain.

For example, disparaging comments against a colleague or client made to all frineds on Facebook could be viewed as bullying/harassment or could be considered to bring the school into disrepute. This could result in disciplinary action being taken against the employee.

Employees are advised to be mindful that all comments made through social media must meed the standards of the Data Protection Act, the Employee Code of Conduct and the Equality and Diversity Policy.

FREEDOM OF INFORMATION (FOI)

Since 1st January 2005, all requests for information received by a public authority have had to be answered in accordance with the Freedom Of Information Act 2000. A school is a public authority. You must be familiar with the basics of the act as any employee could receive a request.

All recorded information held by, or on behalf of a public authority is within the sope of the Act. However, disclosure of personal data is subject to the Data Protection Act. The legislation applies to any recorded information held by the school.

It covers client logs, files, letters, datacases, diairies, loose reports, letters, emails, office notebooks, videos, photographs, wall charts, mapts etc.

It extends to closed files and archived material as well as information in current use. It also extends to social media such as SMS texts, Facebook, Twitter etc *if* it realtes to school business.

If someone makes a written request for general information about the school, contact one of the School Senior Leadership team or the School DPO immediately, who will then allocate the task to the relevant person or department. **The school must respond within 20 working days.**

RECORDS MANAGEMENT

The Records Management Code of Practice states:

- All staff have a legal and professional obligation in respect of any records which they create or use in the performance of their duties
- By records it means files, client logs, minutes, policies, procedures, emails, letters, videos, pictures, web contect etc.
- Any record created in the workplace is an offical record and subject to information requests; FOI, Environmental Information Regulations (EIR) and Subject Access requests (SAR)

This forms part of the School's Retention of Data Policy.

CODE OF PRACTICE

The code of practise covers storing information securely, how long recrds are kept and destryoing when no longer required.

It is important that we:

- Ensure that records are stored securely at all times
- Access to them is controlled
- Dispose of them when they are no longer needed by returning them to the office for shredding

OUR RESPONSIBILITY

It is the responsibility of every employee or person working in a school (be they Governors, Supply staff or volunteers) to be aware of and adhere to the Information Governance Policies.

The name of the School Data Protection Officer is: Mrs Victoria Hardy

The name of the School Safeguarding Leads are: Mrs Joanne Beck, Mrs Louise Schofield and Miss Natalie Tyrrell.