Broadwaters' Inclusive Learning Community

School General Data Protection Policy

May 2018

Document Control

Version History	0.1
Summary of Change	This policy created to reflect best practice or amendments made to the Data Protection Act 1998 by the General Data Protection Regulations.
Implementation date	24th May 2018
Review Date	May 2019
Decision making body & date of approval	Governing body May 2018

Contents

1. Purpose

1.1 The Data Protection legislation (The General Data Protection Regulations (GDPR) and the Data Protection Act 2018) protect individuals with regard to the processing of personal data, in particular by protecting personal privacy and upholding an individual's rights. It applies to anyone who handles or has access to people's personal data.

1.2 This policy is intended to ensure that personal information is dealt with properly and securely and in accordance with the GDPR and the Data Protection Act 2018 (DPA 2018). It will apply to information regardless of the way it is used, recorded and stored and whether it is held in paper files or electronically.

2. Scope

2.1 The GDPR and DPA 2018 have a wider definition of personal data than the Data Protection Act 1998 and includes information generated from cookies and IP addresses if they can identify an individual.

2.2 'Personal data' is any information that relates to an identified or identifiable living individual, which means any living individual who can be identified, directly or indirectly, in particular by reference to—

a. an identifier such as a name, an identification number, location data; or
b. an online identifier; or
c. one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

2.3 The DPA 2018's wider definition of personal data also includes any expression of opinion about an individual, personal data held visually in photographs or video clips (including CCTV) or sound recordings.

2.4 The processing of personal data must be lawful and fair. Under the DPA 2018 "sensitive processing" means the processing of personal data revealing information on an individual that falls under the following:

- Political opinions;
- Religious or philosophical beliefs;
- Trade union membership;
- Genetic data;
- Biometric data;
- Health;
- Sex life;
- Sexual orientation.

2.5 This School collects a large amount of personal data every year including: staff records, names and addresses of those requesting prospectuses, examination marks, references, fee collection as well as the many different types of research data.

2.6 The School may also be required by law to collect and use certain types of information to comply with statutory obligations of Local Authorities (LAs), government agencies (e.g. Department of Education) and other bodies.

2.7 To comply with the Data Protection legislation, this School will collect, use fairly, store safely and not disclose personal data to any other person unlawfully.

3. General Data Protection Principles

3.1 The School needs to demonstrate compliance with six core principles governing processing of personal data:

a. Processing of data is lawful and fair;
b. Purpose is specified, explicit and legitimate (Purpose limitation);
c. The personal data is adequate, relevant and not excessive (Data minimisation);
d. Date processed is accurate and kept up to date (Accuracy);
e. Personal data be kept for no longer than is necessary (Storage limitation);
f. Personal data is processed in a secure manner (Integrity and confidentiality).

3.2 Under the DPA 2018, the wider territorial scope means that the Regulations apply to any Personal Data of any individual who is located in an EEA country irrespective of the country or territory of the organisation processing the data.

3.3 The School will therefore ensure that its contracts with organisations that may process personal data on its behalf are compliant with the Regulations and offer adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

4. Lawful processing

4.1 The School must have a valid lawful basis in order to process personal data.

4.2 The six lawful basis for processing personal data are:

(a) **Consent**: the individual provides clear consent to process their personal data for a specific purpose;
(b) **Contract**: the member of staff/student/parent has given clear consent for the school to process their personal data for a specific purpose, for example, staff employment contract or pupil placement;
(c) **Legal obligation**: the processing is necessary for the School to comply with the law (not including contractual obligations);
(d) **Vital interests**: the processing is necessary to protect someone's life;
(e) **Public task:** the processing is necessary for the School to perform a task in the public interest/official functions, and the task or function has a clear basis in law;

(f) **Legitimate interests:** the processing is necessary for a legitimate interest or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

4.3 The School will generally rely on the following three legal bases for processing data as follows:

(a) Consent;
(b) Contract;
(c) Legal obligation.

4.4 The School will detail its lawful basis for processing personal data in its privacy notice(s).

5. Roles and Responsibilities

Employees

5.1 Every employee, staff member or worker that holds personal information on behalf of the School has to comply with the Data protection Act when managing that information and must treat all personal data in a confidential manner and follow the guidelines as set out in this document.

5.2 All members of the school community are responsible for taking care when handling, using or transferring personal data.

5.3 All members of the school community have a responsibility for ensuring that data cannot be accessed by anyone who does not have permission to access that data.

5.4 Data breaches can have serious effects on individuals and institutions concerned and can bring the School into disrepute. Members of the School community who breach this Policy and/or the Data Protection legislation will be subject to disciplinary action under the School's Disciplinary Policy, which can include sanctions up to and including dismissal. Such breaches may also lead to criminal prosecution.

Pupils over 13 years of age

5.5 Under the DPA 2018, Children aged 13 or over are able to provide their own consent for the processing of their personal data.

5.6 When a child attains 13 years of age, the School will rely on the consent previously provided by the parent(s)/Legal Guardian(s) of the individual.

5.7 If a pupil aged 13 or older wishes to revoke or change the consent previously provided by the pupil's parent(s)/Legal Guardian(s), the individual must suggest and agree with the School a specific agreement on how their data is to be processed.

5.8 Where a pupil is not able to suggest or agree a specific arrangement with the School on how their data is to be processed, the School will continue to process the pupil's data under the parent(s)/legal guardian(s) previously provided consent. The School will inform the pupil of this decision.

5.9 When processing personal data the School will think about the need to protect pupils from the outset, and will consider privacy in its systems and processes during the design stage.

The School - Responsibilities to all data subjects

5.10 The School will ensure that it manages and processes personal data properly; and that protects an individual's right to privacy.

5.11 On request, the School will provide an individual with access to all personal data held on them under a Subject Access Data Request.

5.12 The School has a legal responsibility to comply with the DPA 2018 and the GPDR. The School, as a corporate body, is named as the Data Controller under the DPA 2018.

5.13 The School will consider privacy at the outset and use a data protection by design and by default approach.

5.14 The School will not exploit any imbalance in power in the relationship between the School and its data subjects.

5.15 The School is committed to ensuring that its staff are aware of data protection requirements and legal requirements and will raise awareness of the importance of compliance.

5.16 The requirements of this policy are mandatory for all staff employed by the school and any third party contracted to provide services within the school.

The School - Responsibilities to Pupils

5.17 As a matter of good practice, this School will use Data Protection Impact Assessments (DPIA) to help assess and mitigate data privacy risks to children.

5.18 Where the School processes data that is likely to result in a high risk to the rights and freedom of its pupils it will always complete a DPIA.

5.19 As a matter of good practice, the School will consult with children aged 13 and over as appropriate when designing its processing.

5.20 If the School relies on consent as the lawful reason for processing data it will ensure that children aged 13 or over understand what they are consenting to. The reasons for lawful processing will appear in the School's Privacy Notice.

5.21 When relying on 'necessary for the performance of a contract' as the lawful reason for processing the School will consider the child's competence to understand what they are agreeing to, and to enter into a contract. Where the School believes that a child's competence prohibits informed consent, the School will inform the child of the intention to obtain consent from the child's parent(s)/legal guardian(s). The School will only allow competent children to exercise their own data protection rights.

5.22 Subject to Section 6 below, where the School has relied on consent that was provided by the parent(s)/Legal guardian(s) of the child; when the individual attains 13 years of age the school will comply with request for erasure whenever it can.

5.23 When relying upon 'legitimate interests', we take responsibility for identifying the risks and consequences of the processing, and put age appropriate safeguards in place.

Governors

5.24 Governors are responsible for monitoring the School's compliance with the Regulations.

5.25 Governors may periodically review the DPIAs to assess the School's compliance with the Data Protection legislation.

6. Photographs, video and CCTV images

6.1 Images of staff and pupils may be captured at appropriate times and as part of educational activities for use in school only.

6.2 Unless prior consent from parents/pupils/staff has been given, the School shall not utilise such images for publication or communication to external sources.

6.3 The school will seek consent for photographs and videos for communication, marketing and promotional uses which may include:

- Within school on notice boards and in school magazines, brochures, newsletters, etc.
- Outside of school by external agencies such as the school photographer, newspapers, campaigns
- Online on our school website or social media pages

6.3.1 Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

6.3.2 When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

6.4 It is the School's policy that external parties (including parents) may not capture images of staff or pupils during such activities without prior consent.

6.5 It reflects the ICO's code of practice for the use of surveillance cameras and personal information.

6.5.1 See our [child protection and safeguarding policy/photography policy/other relevant policy] for more information on our use of photographs and videos.

7. Data Security

7.1 The School will use proportionate physical and technical measures to secure personal data.

7.2 The School will consider the security arrangements of any organisation with which data is shared and shall require these organisations to provide evidence of the compliance with the DPA 2018 and GDPR.

7.3 The School will store hard copy data, records, and personal information out of sight and in a locked cupboard. The only exception to this is medical information that may require immediate access during the school day. This will be stored with the School Nurse or designated First Aid Officer.

7.4 Sensitive or personal information and data should not be removed from the school site; however, the School acknowledges that some staff may need to transport data between the school and their home in order to access it for work in the evenings and at weekends. This may also apply in cases where staff have offsite meetings, or are on school visits with pupils.

7.5 To reduce the risk of personal data being compromised any individual taking personal data away from the School site must adhere to the following:

7.5.1 Paper copies of personal data should not be taken off the school site as if misplaced they are easily accessed. If no alternative is available other than to take paper copies of data off the school site then the individual must ensure that the information should not be on view in public places, or left unattended under any circumstances.

7.5.2 Unwanted paper copies of data, sensitive information or pupil files must be shredded. This also applies to handwritten notes if the notes reference any other staff member or pupil by name.

7.5.3 Individuals must take care to ensure that printouts of any personal or sensitive information are not left in printer trays or photocopiers.

7.5.4 Where information is being viewed on a PC, staff must ensure that the window and documents are properly shut down before leaving the computer unattended. Sensitive information should not be viewed on public computers.

7.5.5 Teaching Staff must ensure that personal data and sensitive personal data are not displayed inadvertently on White Boards during class lessons.

7.5.6 If it is necessary to transport data away from the school, it should be downloaded onto a USB stick. The data should not be transferred from this stick onto any home or public computers. Work should be edited from the USB, and saved onto the USB only. USB sticks that staff use must be password protected.

7.5.7 Breaches of the policy will be dealt with in accordance with the School's disciplinary policy and could amount to gross misconduct.

8. Data Retention and Disposal

8.1 The School does not retain personal data or information for longer than it is required, however it is recognised that the School will retain some information on employees and pupils after the individual has left the School.

8.2 The creation of systems and/or files which duplicate such data will be avoided; where it is inevitable every care will be taken to ensure that data maintained in secondary systems is accurate and kept up to date. Disposal of IT assets holding data shall be in compliance with ICO guidance: https://ico.org.uk/media/fororganisations/documents/1570/it_asset_disposal_for_organisations.pdf

9. Data Impact Assessments

9.1 The School will conduct assessments to understand the associated risks of processing personal data that it gather/intends to gather to assist in assuring the protection of all data being processed. The School will use these assessments to inform decisions on processing activities.

9.2 Risk and impact assessments shall be conducted in accordance with guidance given by the ICO: https://ico.org.uk/for-organisations/guide-to-data-protection/principle-7-security/ https://ico.org.uk/for-organisations/guide-to-data-protection/principle-7-security/ https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2014/02/privacyimpact-assessments-code-published/

10. Data Subjects right to be forgotten – Data Erasure

10.1 Data Subjects have the right to request the erasure of their personal data. The School will not comply with a request where the personal data is processed for the following reasons:

- to exercise the right of freedom of expression and information;
- to comply with a legal obligation for the performance of a public interest task or exercise of official authority.
- for public health purposes in the public interest;
- archiving purposes in the public interest, scientific research, historical research or statistical purposes; or
- the exercise or defence of legal claims.

10.2 The School will design its processes so that, as far as possible, it is as easy for a data subject to have their personal data erased as it was for the individual to give their consent in the first place.

11. Data Access Requests (Subject Access Requests)

11.1 All individuals, whose data is held by the School, have a legal right to request access to such data or information about what is held. No charge will be applied to process the request.

11.2 Requests must be made in writing to the Data Protection Officer and the School will respond within one month of receiving the request.

11.3 Personal data about pupils will not be disclosed to third parties without the consent of the child's parent or carer, unless it is obliged by law or in the best interest of the child. Data may be disclosed to the following organisations without consent:

Other schools

11.3.1 If a pupil transfers from The Willow, The Brook or Broadwaters Children's Centre to another school, their academic records and other data that relates to their health and welfare will be forwarded onto the new school.

11.3.2 This will support a smooth transition from one school to the next and ensure that the child is provided for as is necessary. It will aid continuation, which should ensure that there is minimal impact on the child's academic progress because of the move.

Examination authorities

11.3.3 This may be for registration purposes, to allow the pupils at our school to sit examinations set by external exam bodies.

Health authorities

11.3.4 As obliged under health legislation, the school may pass on information regarding the health of children in the school to monitor and avoid the spread of contagious diseases in the interest of public health.

Police and courts

11.3.5 If a situation arises where a criminal investigation is being carried out, the School may have to forward information on to the police to aid their investigation. The School will pass information onto courts as and when it is ordered.

Social workers and support agencies

11.3.6 In order to protect or maintain the welfare of our pupils, and in cases of child abuse, it may be necessary to pass personal data on to social workers or support agencies.

Educational division

11.3.7 The School may be required to pass data on in order to help the government to monitor the national educational system and enforce laws relating to education.

Suppliers and Contractors

11.3.8 Our suppliers or contractors need data to enable us to provide services to our staff, parents /carers and pupils – for example, IT companies. When doing this, we will:

- Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
- Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share
- Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

11.3.9 The Brook, Willow and Broadwaters' Children's Centre may use the suppliers and contractors shown in appendix 2 to enable them to meet their legal obligation as an educational body.

11.3.10 The Data Protection Officer is: Duwan Farquharson

12. Breaches

12.1 The School will notify the individual and the ICO of breaches of personal or sensitive data within 72 hours of becoming aware of the breach.

12.2 In the unlikely event of a suspected data breach, we will follow the procedure set out in appendix 1

13. Notifying the Information Commissioner

13.1 The School is required to 'notify' the Information Commissioner of the processing of personal data. This information will be included in a public register which is available on the Information Commissioner's website at the following link : http://www.ico.gov.uk/what_we_cover/promoting_data_privacy/keeping_the_register.aspx

14. Training

14.1 All staff and governors are provided with data protection training as part of their induction process.

14.2 Data protection will also form part of continuing professional development, where changes to legislation, guidance or the school's processes make it necessary.

15. Monitoring arrangements

15.1 The DPO is responsible for monitoring and reviewing this policy.

15.2 This policy will be reviewed and updated if necessary when the Data Protection Bill receives royal assent and becomes law (as the Data Protection Act 2018) – if any changes are made to the bill that affect our school's practice. Otherwise, or from then on, this policy will be reviewed every 2 years and shared with the full governing board.

16. Further information

16.1 Additional information on the School's Data Protection obligations is located in its Privacy Notice(s).

16.2 The Data Protection Officer is available to provide advice on this policy and information on how the School applies the GPDR and Data Protection Act. See Section 11.3.8 above for the contact details of the DPO.

1. APPENDIX 1: PERSONAL DATA BREACH PROCEDURE

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 DPO
- The DPO will investigate the report, and determine whether a breach has occurred. To decide, the DPO 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 DPO will alert the headteacher and the chair of governors
- The 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. (Actions relevant to specific data types are set out at the end of this procedure)
- The 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 the school's MIS system.
- 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 the School's MIS system 'Cyber Comply'
- The 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 minimise the impact of data breaches

We will take the actions set out below 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.

Sensitive information being disclosed via email (including safeguarding records)

- *If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error*
- *Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error*
- *If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the ICT department to recall it*

- *In any cases where the recall is unsuccessful, the DPO will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way*
- *The DPO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request*
- *The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted*

2. APPENDIX 1: DATA PROCESSORS USED BY THE BROOK, WILLOW AND BROADWATERS' CHILDREN'S CENTRE

Companies	Purposes for Processing Personal Data
Joskos	Manage IT Systems
My Concern	Safeguarding Management Information System
MYCHQ	Manage Extended School Services
PAYPAL	Payment system
E-Start	Management Information System for Children's Centre
Childcare Provider Portal	Management Information System for Childcare and Nursery
LGFL	Manage emails and internet. Also provide educational resources
Target Tracker	Management Information System Attainment data
HCSS	Budgeting Software
Group call Xporter	Provide report to LA on exclusions
Group call	Communication software - Texting services
Evolve	Managed Risk Assessments
Strictly Education	Payroll and HR
School to School Transfer	Transfer data securely to other schools