Contents
1. Aims ................................................................................................................................. 2
2. Legislation and guidance ................................................................................................. 2
3. Definitions .......................................................................................................................... 2
4. The data controller ............................................................................................................ 3
6. Data protection principles ............................................................................................... 4
7. Collecting personal data ................................................................................................... 5
8. Sharing personal data ....................................................................................................... 5
9. Subject access requests and other rights of individuals ................................................. 6
10. Those with parental responsibility requesting to see the educational record .......... 8
11. CCTV ................................................................................................................................ 8
12. Photographs and videos ................................................................................................. 9
13. Data protection by design and default ........................................................................... 9
14. Data security and storage of records ........................................................................... 10
15. Disposal of records ....................................................................................................... 12
16. Personal data breaches .................................................................................................. 12
17. Training ........................................................................................................................... 13
18. Monitoring arrangements ............................................................................................... 13
19. Links with other policies .............................................................................................. 13
20. Appendix 1 : DPO job description .............................................................................. 14
21. Appendix 2: Personal data breach procedure ......................................................... 15
23. Appendix 4 : Data Breach Report Form ..................................................................... 21
1. Aims

Our school aims to ensure that all data collected about staff, children/young people, people with parental responsibility and visitors is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill.

This policy applies to all data, regardless of whether it is in paper or electronic format.

2. Legislation and guidance

This policy meets the requirements of the GDPR and the expected provisions of the DPA 2018. It is based on guidance published by the Information Commissioner’s Office (ICO) on the GDPR and the ICO’s code of practice for subject access requests.

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

In addition, this policy complies with regulation 5 of the Education (Pupil Information) (England) Regulations 2005, which gives those with parental responsibility the right of access to their child/young person’s educational record.

3. Definitions

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Personal data</td>
<td>Any information relating to an identified, or identifiable, individual. This may include the individual’s:</td>
</tr>
<tr>
<td></td>
<td>• Name (including initials)</td>
</tr>
<tr>
<td></td>
<td>• Identification number</td>
</tr>
<tr>
<td></td>
<td>• Location data</td>
</tr>
<tr>
<td></td>
<td>• Online identifier, such as a username</td>
</tr>
<tr>
<td></td>
<td>It may also include factors specific to the individual’s physical, physiological, genetic, mental, economic, cultural or social identity.</td>
</tr>
<tr>
<td>Special categories of personal data</td>
<td>Personal data which is more sensitive and so needs more protection, including information about an individual’s:</td>
</tr>
<tr>
<td></td>
<td>• Racial or ethnic origin</td>
</tr>
<tr>
<td></td>
<td>• Political opinions</td>
</tr>
<tr>
<td></td>
<td>• Religious or philosophical beliefs</td>
</tr>
<tr>
<td></td>
<td>• Trade union membership</td>
</tr>
</tbody>
</table>
### Genetics
- Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes
- Health – physical or mental
- Sex life or sexual orientation

| **Processing** | Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual. |
| **Data subject** | The identified or identifiable individual whose personal data is held or processed. |
| **Data controller** | A person or organisation that determines the purposes and the means of processing of personal data. |
| **Data processor** | A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller. |
| **Personal data breach** | A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data. |

#### 4. The data controller

Our school processes personal data relating to people with parental responsibility, children/young people, staff, governors, visitors and others, and therefore is a data controller.

The school is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

#### 5. Roles and responsibilities

This policy applies to all staff employed by our school, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

#### 5.1 Governing body

The governing body has overall responsibility for ensuring that our school complies with all relevant data protection obligations.
5.2 Data protection officer
The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

The DPO is also the first point of contact for individuals whose data the school processes, and for the ICO.

Full details of the DPO’s responsibilities are set out in their job description (See Appendix 1).

Our DPO is Mr Gary Hipple and is contactable via ghipple@wandsworth.gov.uk.

5.3 Head teacher
The head teacher acts as the representative of the data controller on a day-to-day basis.

5.4 All staff
Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the school of any changes to their personal data, such as a change of address
- Contacting the DPO in the following circumstances:
  - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
  - If they have any concerns that this policy is not being followed
  - If they are unsure whether or not they have a lawful basis to use personal data in a particular way
  - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
  - If there has been a data breach
  - Whenever they are engaging in a new activity that may affect the privacy rights of individuals
  - If they need help with any contracts or sharing personal data with third parties

6. Data protection principles
The GDPR is based on data protection principles that our school must comply with. The principles say that personal data must be:

1. Processed lawfully, fairly and in a transparent manner
2. Collected for specified, explicit and legitimate purposes
3. Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
4. Accurate and, where necessary, kept up to date
5. Kept for no longer than is necessary for the purposes for which it is processed
6. Processed in a way that ensures it is appropriately secure
This policy sets out how the school aims to comply with these principles.

7. Collecting personal data

7.1 Lawfulness, fairness and transparency
We will only process personal data where we have one of 6 ‘lawful bases’ (legal reasons) to do so under data protection law:

- The data needs to be processed so that the school can fulfil a contract with the individual, or the individual has asked the school to take specific steps before entering into a contract
- The data needs to be processed so that the school can comply with a legal obligation
- The data needs to be processed to ensure the vital interests of the individual e.g. to protect someone’s life
- The data needs to be processed so that the school, as a public authority, can perform a task in the public interest, and carry out its official functions
- The data needs to be processed for the legitimate interests of the school or a third party (provided the individual’s rights and freedoms are not overridden)
- The individual (or the person with parental responsibility when appropriate in the case of a child/young person) has freely given clear consent

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018.

If we offer online services to pupils, such as classroom apps, and we intend to rely on consent as a basis for processing, we will get parental consent where the child is under 13. If the child/young person is aged 13 and above we may get their consent, as considered appropriate.

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

7.2 Limitation, minimisation and accuracy
We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs.

When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with guidance from the Information and Records Management Society’s toolkit for schools.

8. Sharing personal data
We will not normally share personal data with anyone else, but may do so where:

- There is an issue with a child/young person or person with parental responsibility that puts the safety of our staff at risk
• We need to liaise with other agencies – we will seek consent as necessary before doing this.

• Our suppliers or contractors need data to enable us to provide services to our staff and children/young people – for example, IT companies. When doing this, we will:
  o Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
  o 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
  o 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

We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

• The prevention or detection of crime and/or fraud
• The apprehension or prosecution of offenders
• The assessment or collection of tax owed to HMRC
• In connection with legal proceedings
• Where the disclosure is required to satisfy our safeguarding obligations
• Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or staff.

Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

9. Subject access requests and other rights of individuals

9.1 Subject access requests (SAR)
Individuals have a right to make a ‘subject access request’ to gain access to personal information that the school holds about them. This includes:

• Confirmation that their personal data is being processed
• Access to a copy of the data
• The purposes of the data processing
• The categories of personal data concerned
• Who the data has been, or will be, shared with
• How long the data will be stored for, or if this isn’t possible, the criteria used to determine this period
• The source of the data, if not the individual
• Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

Subject access requests must be submitted in writing, either by letter, email or fax to the School.
Business Manager. They should include:

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested

If staff receive a subject access request they must immediately forward it to the School Business Manager [See Appendix 3].

9.2 Children and subject access requests

Personal data about a child belongs to that child, and not the person with parental responsibility for the child. For a person with parental responsibility for the child to make a subject access request with respect to the child they have responsibility for, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from a person with parental responsibility for the child may be granted without the express permission of the child. This is not a rule and a child’s ability to understand their rights will always be judged on a case-by-case basis.

Children/young people aged 12 and above can generally be regarded as able enough to understand their rights and the implications of a subject access request, dependent on the child/young person. Therefore, subject access requests from person with parental responsibility for the child/young person at our school may not be granted without the express permission of the child/young person. This is not a rule and a pupil’s ability to understand their rights will always be judged on a case-by-case basis.

9.3 Responding to subject access requests

When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request
- Will provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the child/young person or another individual
- Would reveal that the child/young person is at risk of abuse, where the disclosure of that information would not be in the child/young person’s best interests
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning the child/young person

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee
which takes into account administrative costs.

A request will be deemed to be unfounded or excessive if it is repetitive, or asks for further copies of the same information. When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

9.4 Other data protection rights of the individual
In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see section 7), individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

10. Those with parental responsibility requesting to see the educational record

Those with parental responsibility, have a legal right to free access to their child’s educational record (which includes most information about a pupil) within 15 school days of receipt of a written request.

11. CCTV

We use CCTV in various locations around the school site to ensure child/young person safety and help prevent crime. We will adhere to the ICO’s code of practice for the use of CCTV. We do not need to ask individuals’ permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

Any enquiries about the CCTV system should be directed to the School Business Manager. [Please also refer to separate CCTV Policy]
12. Photographs and videos

As part of our school activities, we may take photographs and record images of individuals within our school. We will obtain written consent from those with parental responsibility, or young people aged 18 and over, as appropriate, for photographs and videos to be taken of young people for communication, marketing and promotional materials, etc.

Where we need consent from those with parental responsibility, we will clearly explain how the photograph and/or video will be used to both those with parental responsibility and the young person, as appropriate. Where we don’t need parental consent, we will clearly explain to the young person how the photograph and/or video will be used.

Uses may include:

- Videoed by the school for use in class and home to assist with reflective practice for staff (Commitment to Gentle Teaching: we use videos to reflect on behaviour support and staff skills).
- Videoed by the speech and language therapy department for assessments, observations and during training sessions for internal and external staff.
- Videoed / photographed by the school for their personalised Wiki
- Photographed by the school for use in class and team work (e.g. communication boards and internal displays).
- Photographed for use in our forthcoming prospectus.
- Photographed by the school for use on the website.
- Photographs used in local press i.e. school events.
- Videoed by the school during school productions that may be used on the school website and for external presentations.
- Videoed during assemblies and other school activities so that individual DVD’s can be shared with parents/carers

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.

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.

13. Data protection by design and default

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)
- Completing privacy impact assessments where the school’s processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
• Integrating data protection into internal documents including this policy, any related policies and privacy notices
• Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
• Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
• Maintaining records of our processing activities, including:
  o For the benefit of data subjects, making available the name and contact details of our school and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
  o For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure

14. Data security and storage of records

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

Strategic and operational practices

At this school:

• The School Business Manager is the Senior Information Risk Officer (SIRO).
• Gary Hipple is the Data Protection Officer (DPO) with responsibility for data protection compliance.
• Staff are clear who the key contacts for key school information are (the Information Asset Owners). We have listed the information and information asset owners in a spreadsheet called ‘GDP data audit log’.
• 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 on SIMS

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

  o staff
  o governors
  o pupils
  o parents
  o 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 also have an additional layer of monitoring software across our network system called Impero. We monitor school e-mails, etc to ensure compliance with the Acceptable Use Agreement. As well as monitoring usage, we may also monitor content of e-mails, etc.

• 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. Network logon password change by staff every 120 days is enforced by server logon policy.

• We require staff to use strong passwords for access into our MIS system.

• Nominated contact staff to change their passwords into the USO admin site every 90 days and makes use of second factor authentication. (This is enforced by Atomwide, the LGfL provider)

• We require that any personal/sensitive material must be encrypted if the material is to be removed from the school, and limit such data removal. We have an approved remote access solution so staff can access sensitive and other data from home, without need to take data home.

Technical or manual solutions

• Staff have secure areas on the network to store sensitive documents or photographs.

• We require admin staff to log-out of systems when leaving their computer, but also enforce lock-out after 15 mins. idle time.

• We use encrypted flash drives if any member of staff has to take any sensitive information off site.

• We use RAv3 / VPN solution for remote access into our systems.

• 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 services and online resources.

• All staff use LGfL staffmail for all school related email. This ensures staff-to-staff email is encrypted by default

• We use LGfL's USO-FX2 to transfer documents to schools in London, such as references, reports of children.

• We store any sensitive/special category written material in lockable storage cabinets in a lockable storage area/office.

• All servers are in lockable locations and managed by DBS-checked staff.

• All backup drives are stored in secure, locked locations.

• 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 an approved data disposal contractor.

• Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use.

• Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access.

• Where possible, all storage devices that contain sensitive data must be encrypted. This will be implemented when Windows 10 devices are rolled out in the near future.

• Staff, children/young people or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment (see our ICT acceptable use policy). E.g. Staff using their own personal devices for school emails (LGFL provided StaffMail), which may potentially contain sensitive school information, must ensure they password protect their device.

• Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8).

• Emails containing sensitive data must be encrypted using Egress Switch encryption software. This includes email between staff as the email gets sent outside the school and back in again.

• Data held on our servers and network attached storage are backed up daily to separate storage on another part of the school site.

• Anti-virus software is used on all computers and is freely available for staff to install on their home computers.

• Staff must not transfer/store any school data (pupil/staff info/photos/videos, etc) to any Cloud service, e.g. DropBox, ICloud, Google Drive, Microsoft OneDrive, etc apart from the LGFL provided O365 Cloud storage (which complies with the Data Protection Act, as data is stored in the EU).

15. Disposal of records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the school’s behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

16. Personal data breaches

The school will make all reasonable endeavours to ensure that there are no personal data breaches. In the unlikely event of a suspected data breach, we will follow the procedure set out in appendix 2. See also Data Breach Report from in Appendix 4.
When appropriate, we will report the data breach to the ICO within 72 hours. Such breaches in a school context may include, but are not limited to:

- Safeguarding information being made available to an unauthorised person
- The theft of a school laptop containing non-encrypted personal data about children/young people

### 17. Training

All staff and governors are provided with data protection training as part of their induction process. Data protection will also form part of continuing professional development, where changes to legislation, guidance or the school’s processes make it necessary.

### 18. Monitoring arrangements

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

*Note: the 2-year review frequency here reflects the information in the Department for Education’s advice on statutory policies. While the GDPR and Data Protection Act 2018 (when in place) are still new and schools are working out how best to implement them, you may wish to review your data protection policy annually, and then extend this to every 2 years once you are confident with your arrangements.*

### 19. Links with other policies

This data protection policy is linked to our:

- Freedom of information publication scheme
- ICT acceptable use policy
- Online safety policy
- Child protection and safeguarding policy
- CCTV Policy
20. Appendix 1: DPO job description

<table>
<thead>
<tr>
<th>Job Title: Schools Data Protection Officer</th>
<th>Directorate: Education, performance &amp; planning, Schools ICT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Responsible to following manager: Gary Hipple</td>
<td></td>
</tr>
</tbody>
</table>

**Job Purpose**

- To fulfil the legal role of Data Protection Officer for Schools.
- To champion data protection and privacy in schools, including raising awareness of the importance of effective practice and consequences of non-compliance.

**Specific Duties and Responsibilities**

- Develop an in depth understanding of Schools processing operations, information systems, data security processes and needs
- Devise and deliver a programme of work for schools in compliance with the GDPR, including a gap analysis of the School’s policies and procedures
- Review and monitor compliance with Data Protection legislation and data protection policies, including spot check and audits
- Support school’s development of an Information Asset Register and implement a process to ensure the ongoing maintenance of the Asset Register as part of any ongoing development processes
- Undertake and advise on data protection impact assessments and monitor existing projects
- Inform and advise the School/organisation and staff who process personal data of their obligations
- Monitor changes in data protection law and regulations and recommend relevant updates to policies, processes and procedures, including drafting appropriate amendments where requested
- To liaise with the Council’s corporate data protection staff for sharing of development and training and consistency of best practice.
- Design and deliver data protection training and guidance to staff to increase school wide awareness of the GDPR and staff capability to comply with the Regulation
- To lead for all schools on any data breach investigations and notifications
- Develop a strategy for a Data Protection by Design approach for the School or organisation
- Advise senior staff (i.e. Headteachers, Deputy Heads, Senior Leadership Teams, and Governing Bodies in Schools or Senior Managers, Senior Management Teams, Board Members etc) on Data Protection issues, significant risks and incidents
21. Appendix 2: 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 School Business Manager (SBM).
- The SBM 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 SBM will alert the headteacher and the chair of governors
- The SBM 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 SBM will assess the potential consequences, based on how serious they are, and how likely they are to happen
- The SBM 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 SBM 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 SBM must notify the ICO.

- The SBM 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 computer system.
- Where the ICO must be notified, the SBM will do this via the ‘report a breach’ page of the ICO website within 72 hours. As required, the SBM 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 SBM and 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 SBM 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 SBM expects to have further information. The SBM will submit the remaining information as soon as possible.
• The SBM 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 SBM will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
  o The name and contact details of the DPO
  o A description of the likely consequences of the personal data breach
  o 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 SBM 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 SBM will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
  o Facts and cause
  o Effects
  o 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 [set out where you will keep these records – for example, on the school’s computer system, or on a designated software solution]

• The SBM 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.

Data Breach potential scenario:

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 SBM as soon as they become aware of the error

• If the sender is unavailable or cannot recall the email for any reason, the SBM will ask the ICT department to recall it

• In any cases where the recall is unsuccessful, the SBM 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 SBM will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request

The SBM 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
22. Appendix 3: Subject Access Request procedure

Scope
All personal data processed by Bradstow School or on behalf of Bradstow School is within the scope of this procedure.

Data subjects are entitled to obtain:
- Confirmation as to whether Bradstow School is processing any personal data about that individual;
- Access to their personal data;
- Any related information;

Procedure
Subject Access Requests (SARs) for information must be made in writing and sent to the School Business Manager. The school will provide a template for the request (See within this appendix). If an individual is unable to provide a request in writing and justifiable assistance is required, it must be provided and the request can be made on behalf of the individual. Bradstow School does not need to respond to a request made orally but, depending on the circumstances, it might be reasonable to do so (as long as Bradstow School is satisfied about the person’s identity). It is good practice at least to explain to the individual how to make a valid request, rather than ignoring them. If a request does not mention the Data Protection Legislation specifically or even say that it is a subject access request, it is nevertheless valid and should be treated as such if it is clear that the individual is asking for their own or child’s personal data.

Requesters do not have to tell Bradstow School their reason for making the request or what they intend to do with the information requested, although it may help to find the relevant information if they do explain the purpose of the request.

A request is valid even if the individual has not sent it directly to the person who normally deals with such requests. So it is important to ensure you recognise a subject access request (SAR) and forward it to the named person in school who will liaise with the school Data Protection Officer. Any school employee who receives a request for a subject access request (SAR) must forward it immediately to the School Business Manager, no matter what form it is received in. The School Business Manager will log and acknowledge the request.

The data subject will provide the school with evidence of their identity and the signature on the identity must be cross-checked.
List of acceptable identity includes:
- Passport
- Driving licence
- Birth certificate
- Utility bill (from last 3 months)
- Current vehicle registration document
- Bank statement (from last 3 months)
- Rent book (from last 3 months)
- Council tax

The data subject may specify to Bradstow School a specific set of data held by Bradstow School on their subject access request (SAR). The data subject can request all data held on them. The School Business Manager will update the log and record the date that the identification checks were conducted and the specification of the data sought.
The School Business Manager will work with the school Data Protection Officer to provide the requested information to the data subject within one month from this recorded date.

Under the GDPR Article 12 (3), the month deadline may be extended by two further months where necessary, taking into account the complexity and number of the requests.

The School Business Manager shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay.

Example of reason for the delay:
- Volume of information is over 1,000 pages
- Open complex cases
- Three or more third parties are included

Where the data subject makes the request by electronic means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject.

Once received, the subject access request (SAR) is immediately forwarded to the School Business Manager, who will ensure that the requested data is collected within the specified time frame.

Collection entails:
- Collecting the data specified by the data subject,
- Request Bradstow School to search and retrieve information from all relevant databases and all relevant filing systems (manual files) in the school, including all back up and archived files (computerised or manual) and all email folders and archives.

The Data Protection Officer will maintain a record of requests for data and of its receipt, including dates and copies of correspondences.

All documents should be reviewed that have been provided, to identify whether any third parties are present in it, and either remove the identifying third party information from the documentation or obtain written consent from the third party for their identity to be revealed.

The DPA currently sets out a number of exemptions which allow information to be withheld from data subjects in circumstances in which it would otherwise need to be disclosed.

Current exemptions which are relevant include:
- Confidential references – schools do not have to provide subject access to references they have confidentially given in relation to an employee’s employment;
- Management information – personal data which relates to management forecasting or planning is exempt from subject access (to the extent complying with the SAR would be likely to prejudice the business activity of the organisation);
- Legal advice and proceedings – schools do not have to disclose data which is covered by legal professional privilege;
- Settlement negotiations – the subject is not entitled to personal data which consists of a record of the employers intentions in respect of settlement discussions that have taken place or are in the process of taking place with that individual.

In the event that a data subject requests details of what personal data is being processed then they should be provided with the following information:

- Purpose of the processing
- Categories of personal data
• Recipient(s) of the information, including recipients in third countries or international organisations
• How long the personal data will be stored
• The data subject’s right to request rectification or erasure, restriction or objection, relative to their personal data being processed.
• Bradstow School takes appropriate measures to act without undue delay in the event that the data subject has: withdrawn consent (objects to the processing of their personal data in whole or part; no longer under legal obligation and/or has been unlawfully processed.

Inform the data subject of their right to lodge a complaint with the ICO and a method to do so.

Inform the data subject of any automated decision-making.

If and where personal data has been transferred and information on any safeguards in place.

Bradstow School does not charge a fee for Subject Access Requests (SARs).

**Complaints against Subject Access Requests (SARs)**

Individuals that wish to make a complaint about the handling of their Subject Access Request (SAR) can raise a concern with the Data Protection Officer. They also have a right to raise their concern with the Information Commissioner’s Office. Any Subject Access Request (SAR) concern received by a school employee must be forwarded to the Data Protection Officer immediately.
**Form For Submitting Subject Access Requests**

Schools: Bradstow School, 34 Dumpton Park Drive, Broadstairs, Kent CT10 1BY

Date: ______________________

**Re: subject access request**

Dear Bradstow School:

Please provide me with the information about me that I am entitled to under the Data Protection Act 2018 and General Data Protection Regulation (GDPR). This is so I can be aware of the information you are processing about me, and verify the lawfulness of the processing.

Here is the necessary information:

<table>
<thead>
<tr>
<th>Name</th>
<th>Relationship with the school</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Please select:</td>
</tr>
<tr>
<td></td>
<td>Pupil / parent / employee / governor / volunteer</td>
</tr>
<tr>
<td></td>
<td>Other (please specify):</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Correspondence address</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Contact number</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Email address</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Details of the information requested</th>
</tr>
</thead>
</table>

Please provide me with:

*Insert details of the information you want that will help us to locate the specific information. Please be as precise as possible, for example:*

- Your personnel file
- Your child’s medical records
- Your child’s behavior record, held by [insert class teacher]
- Emails between ‘A’ and ‘B’ between [date]

If you need any more information from me, please let me know as soon as possible.

Please bear in mind that under the GDPR you cannot charge a fee to provide this information, and in most cases, must supply me with the information within 1 month.

If you need any advice on dealing with this request, you can contact the Information Commissioner’s Office on 0303 123 1113 or at [www.ico.org.uk](http://www.ico.org.uk)

Yours sincerely,

Name
### Data Breach Reporting Form

Please complete the form below to notify the Data Protection Officer of a data protection breach. Please email to Gary Hipple ghipple@wandsworth.gov.uk

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Summary of the event and circumstances:</td>
</tr>
<tr>
<td>2</td>
<td>Type and amount of data (personal/staff, student, parental/carer):</td>
</tr>
<tr>
<td>3</td>
<td>Actions taken to retrieve the information and minimise the effect of the breach:</td>
</tr>
<tr>
<td>4</td>
<td>Details of notification to affected data subject: (if applicable)</td>
</tr>
<tr>
<td></td>
<td>Has a complaint been received from the affected data subject?</td>
</tr>
<tr>
<td>5</td>
<td>Breach of procedure / policy by staff member:</td>
</tr>
<tr>
<td>6</td>
<td>Details of Data Protection training provided/taken:</td>
</tr>
<tr>
<td>7</td>
<td>Any procedure changes required to reduce risks of future data loss:</td>
</tr>
<tr>
<td>8</td>
<td>Conclusion:</td>
</tr>
</tbody>
</table>