DATA PROTECTION, GDPR, PRIVACY NOTICE AND SUBJECT ACCESS REQUEST POLICY 2023-2025

The Lady Byron School

Written by:	Caroline England	**Date:** July 2024
Approved by:	Alison Siddons	**Date:** July 2024
Last reviewed on:	August 2024	
Next review due by:	August 2025	

Table of Contents

1. Data protection and GDPR Aims

1.1 The Lady Byron School aims to ensure that all personal data collected about staff, pupils, parents, visitors and other individuals 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.

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

2. Legislation and Guidance

2.1 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.

2.2 In addition, this policy complies with regulation 5 of the Education (Pupil Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record.

3. Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, individual. This may include the individual's: • Name (including initials) • Identification number • Location data • Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.

Special categories of personal data	Personal data, which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • 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

4.1 The Lady Byron School processes personal data relating to parents, pupils, staff, 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

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

5.2 Proprietor
The Proprietor has overall responsibility for ensuring that The Lady Byron School complies with all relevant data protection obligations.

5.3 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.

5.4 They will provide an annual report of their activities directly to the Proprietor and, where relevant, report to the board their advice and recommendations on school data protection issues.

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

5.6 Full details of the DPO's responsibilities are set out in their job description.

5.7 Our DPO is Alison Siddons and is contactable via email reception@ladybyronschool.co.uk

5.8 Headteacher

5.9 The headteacher acts as the representative of the data controller on a day-to-day basis.

5.10 All staff

5.11 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

6.1 The GDPR is based on data protection principles that The Lady Byron School must comply with.

6.2 The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

6.3 This policy sets out how the school aims to comply with these principles.

7. Collecting personal data

7.1 Lawfulness, fairness and transparency

7.2 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 their parent/carer when appropriate in the case of a pupil) has freely given clear consent

7.3 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.

7.4 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 pupil is under 13 (except for online counselling and preventive services).

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

7.6 Limitation, minimisation and accuracy

7.7 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.

7.8 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.

7.9 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 the school's Information and Records Management Society's toolkit for schools https://irms.org.uk/page/SchoolsToolkit

8. Sharing personal data

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

- There is an issue with a pupil or parent/carer 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 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

8.2 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

8.3 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.

8.4 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

9.2 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

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

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

9.4 If staff receive a subject access request, they must immediately forward it to the DPO.

9.5 Children and subject access requests

9.6 Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request or have given their consent.

9.7 Children aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at The Lady Byron School may not be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

9.8 Responding to subject access requests

9.9 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

9.10 We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests

- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning the child

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

9.12 A request will be deemed to be unfounded or excessive if it is repetitive or asks for further copies of the same information.

9.13 When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

9.14 Other data protection rights of the individual

9.15 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)

9.16 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. Parental requests to see the educational record

10.1 Parents, or 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. Photographs and videos

11.1 As part of The Lady Byron School activities, we may take photographs and record images of individuals within our school.

11.2 We will obtain written consent from parents/carers, or pupils aged 18 and over, for photographs and videos to be taken of pupils for communication, marketing and promotional materials.

11.3 Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil. Where we don't need parental consent, we will clearly explain to the pupil how the photograph and/or video will be used.

11.4 Uses 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 The Lady Byron School website or social media pages

11.5 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.

11.6 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.

11.7 See our child protection and safeguarding policy for more information on our use of photographs and videos.

12. Data protection by design and default

12.1 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: https://ico.org.uk/for-organisations/
- 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:
    - For the benefit of data subjects, making available the name and contact details of The Lady Byron School and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
    - 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

13. Data security and storage of records

13.1 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.

13.2 In particular:

- 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 personal information needs to be taken off site, staff must sign it in and out from the school office
- Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- Staf for pupils who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment (see our [online safety policy/ICT policy/acceptable use agreement/policy on acceptable use])
- 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)

14. Disposal of records

14.1 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.

14.2 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.

15. Personal data breaches

15.1 The school will make all reasonable endeavours to ensure that there are no personal data breaches.

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

15.3 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:

- A non-anonymised dataset being published on the school website which shows the exam results of pupils eligible for the pupil premium
- Safeguarding information being made available to an unauthorised person
- The theft of a school laptop containing non-encrypted personal data about pupils

16. Training

16.1 All staff are provided with data protection training as part of their induction process.

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

17. Monitoring arrangements

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

17.2 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 The Lady Byron School's practice. Otherwise, or from then on, this policy will be reviewed every 2 years and shared with the staff.

18. Links with other policies

18.1 This data protection policy is linked to our:

- Freedom of information publication scheme
- E-safety policy
- Safeguarding Policy

19. Privacy notice for parents/carers – use of your child's personal data

19.1 Under data protection law, individuals have a right to be informed about how the school uses any personal data that we hold about them. We comply with this right by providing 'privacy notices' (sometimes called 'fair processing notices') to individuals where we are processing their personal data.

19.2 We, The Lady Byron School, are the 'data controller' for the purposes of data protection law. This privacy notice also covers data held at and for The Lady Byron School, The Cedars, 11 High Street, Fleckney Leicestershire. LE8 8AJ.

19.3 The data protection officer for The Lady Byron School is Martine Browne. (see 'Contact us' below).

19.4 The personal data we hold

19.5 Personal data that we may collect, use, store and share (when appropriate) about pupils includes, but is not restricted to:

- Contact details, contact preferences, date of birth,
- Results of internal assessments and externally set tests
- Pupil and curricular records
- Characteristics, such as ethnic background, eligibility for free school meals, or special educational needs
- Details of any medical conditions, including physical and mental health
- Attendance information
- Safeguarding information
- Details of any support received, including plans and support providers
- Photographs
- Video recordings
- Information relating to incidents, injuries and behaviour support

19.6 We may also hold data about pupils that we have received from other organisations, including other schools, local authorities and the Department for Education.

19.7 Why we use this data

19.8 We use this data to:

- Support pupil learning
- Monitor and report on pupil progress
- Provide appropriate pastoral care
- Protect pupil welfare
- Assess the quality of our services
- Administer admissions
- Carry out research
- Comply with the law regarding data sharing

20. Our legal basis for using this data

20.1 We only collect and use pupils' personal data when the law allows us to. Most commonly, we process it where:

- We need to comply with a legal obligation
- We need it to perform an official task in the public interest

20.2 Less commonly, we may also process pupils' personal data in situations where:

- We have obtained consent to use it in a certain way
- We need to protect the individual's vital interests (or someone else's interests)

20.3 Where we have obtained consent to use pupils' personal data, this consent can be withdrawn at any time. We will make this clear when we ask for consent and explain how consent can be withdrawn.

20.4 Some of the reasons listed above for collecting and using pupils' personal data overlap, and there may be several grounds which justify our use of this data.

21. Collecting this information

21.1 While the majority of information we collect about pupils is mandatory, there is some information that can be provided voluntarily.
Whenever we seek to collect information from you or your child, we make it clear whether providing it is mandatory or optional. If it is mandatory, we will explain the possible consequences of not complying.

22. How we store this data

22.1 We keep personal information about pupils while they are attending The Lady Byron School. We may also keep it beyond their attendance at our school if this is necessary in order to comply with our legal obligations. The Information and Records Management Society's toolkit for schools sets out how long we keep information about pupils. A copy of this is available from the school office.

23. Data sharing

23.1 We do not share information about pupils with any third party without consent unless the law and our policies allow us to do so.
Where it is legally required, or necessary (and it complies with data protection law) we may share personal information about pupils with:

- The child's local authority – to meet our legal obligations to share certain
- information with it, such as safeguarding concerns and exclusions
- The Department for Education – we are required by law to provide information
- about our pupils to the DfE as part of statutory data collections such as the
- school census.
- The pupil's family and representatives
- Educators and examining bodies
- Our regulator Ofsted
- Other inspecting bodies
- Suppliers and service providers – to enable them to provide the service we have contracted them for
- Health authorities
- Health and social welfare organisations
- Professional advisers and consultants
- Charities and voluntary organisations
- Police forces, courts, tribunals
- Professional bodies

24. National Pupil Database

24.1 We are required to provide information about pupils to the Department for Education as part of statutory data collections such as the school census. Some of this information is then stored in the National Pupil Database (NPD), which is owned and managed by the Department and provides evidence on school performance to inform research.

24.2 The database is held electronically so it can easily be turned into statistics. The information is securely collected from a range of sources including schools, local authorities and exam boards.
The Department for Education may share information from the NPD with other organisations which promote children's education or wellbeing in England. Such organisations must agree to strict terms and conditions about how they will use the data.

24.3 For more information, see the Department's webpage on how it collects and shares research data.

24.4 You can also contact the Department for Education with any further questions about the NPD.

25. Youth support services

25.1 Once our pupils reach the age of 13, we are legally required to pass on certain information about them to our local Connexions service, as they have legal responsibilities regarding the education or training of 13–19-year-olds.

25.2 This information enables it to provide youth support services, post-16 education and training services, and careers advisers.

25.3 Parents/carers, or pupils once aged 16 or over, can contact our data protection officer to request that we only pass the individual's name, address and date of birth to Connexions.

26. Transferring data internationally

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

27. Parents and pupils' rights regarding personal data

27.1 Individuals have a right to make a 'subject access request' to gain access to personal information that the school holds about them.

27.2 Parents/carers can make a request with respect to their child's data where the child is not considered mature enough to understand their rights over their own data (usually under the age of 12), or where the child has provided consent. We will consider a child's level of understanding, mental capacity and their best interests when considering whether to provide the data requested to yourself or your child.

27.3 If you make a subject access request, and if we do hold information about you or your child, we will:

- Give you a description of it
- Tell you why we are holding and processing it, and how long we will keep it for
- Explain where we got it from, if not from you or your child
- Tell you who it has been, or will be, shared with
- Let you know whether any automated decision-making is being applied to the data, and any consequences of this
- Give you a copy of the information in an intelligible form

27.4 Individuals also have the right for their personal information to be transmitted electronically to another organisation in certain circumstances. If you would like to make a request please contact our data protection manager.

28. Other rights

28.1 Under data protection law, individuals have certain rights regarding how their personal data is used and kept safe, including the right to:

- Object to the use of personal data if it would cause, or is causing, damage or distress
- Prevent it being used to send direct marketing

- Object to decisions being taken by automated means (by a computer or machine, rather than by a person)
- In certain circumstances, have inaccurate personal data corrected, deleted or destroyed, or restrict processing
- Claim compensation for damages caused by a breach of the data protection regulations

28.2 To exercise any of these rights, please contact our data protection manager or officer.

29. Complaints

29.1 We take any complaints about our collection and use of personal information very seriously. If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concern about our data processing, please raise this with us in the first instance.

29.2 To make a complaint, please contact our data protection manager or officer. Alternatively, you can make a complaint to the Information Commissioner's Office:

- Report a concern online at: https://ico.org.uk/make-a-complaint/
- Call: 0303 123 1113

30. Contact us

30.1 If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact our data protection officer via the school.

30.2 Data Protection Officer – Martine Browne

30.3 This notice is based on the Department for Education's model privacy notice for pupils, amended for parents and to reflect the way we use data in this school.

31. Subject Access Request- Process and Protocol

31.1 As an organisation we collect and process data about individuals. We explain what information we collect, and why in our Privacy Notices

31.2 Any individual, or person with parental responsibility, or young person with sufficient capacity to make a request is entitled to ask what information is held. Copies of the information shall also be made available on request. A form to complete is available.

31.3 To ensure that requests are dealt with in an effective and timely manner we may seek to clarify the terms of a request.

31.4. Please ensure that requests are made in writing to the DCO.

31.5 Evidence of their identity, on the basis of the information set out and the signature on the identity must be cross-checked to that on the application form. Discretion about employees and persons known to the school may be applicable but if ID evidence is not required an explanation must be provided by school staff and signed and dated accordingly

32. Exemptions to a SAR exist and may include

32.1

- Education, Health, Social Work records
- Examination marks and scripts
- Safeguarding records
- Special educational needs
- Parental records and reports
- Legal advice and proceedings
- Adoption and Court records and/or reports
- Regulatory activity and official requests e.g. DfE statistical information
- National security, Crime and taxation
- Journalism, literature and art
- Research history, and statistics
- Confidential references

33. All data subjects have the right to know: -

33.1

- What information is held?
- Who holds it?
- Why is it held?
- What are the retention periods?
- That each data subject has rights. Consent can be withdrawn at any time (to some things).
- A right to request rectification, erasure or to limit or stop processing
- A right to complain

33.2 Many of these questions will be within the Privacy Notices on the website.

33.3 The information will be provided in an electronic format, usually within one calendar month of the request. However, in some circumstances, for example the school is closed for holidays, this may be extended by up to another calendar month.

34. Version History

34.1 This policy was last reviewed in August 2024

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 Proprietor
- 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 computer 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
    - 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 computer system. 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

Appendix 2

The Lady Byron School (LBS) subject access request form: parental request on behalf of a child

General Data Protection Regulation – Subject Access Request Form for people with parental responsibility acting on behalf of a child

The General Data Protection Regulation (GDPR) gives individuals the right to receive a copy of the data/information we hold about them. There are special rules about children and people who have parental responsibility for children. Please read the following sections carefully if you want to make a subject access request on behalf of a child for whom you have parental responsibility[1]

Children who are of sufficient age, maturity and ability to make a request are treated in the same way as adults. For these children, the child alone has the right to ask for and see their personal data. As a general rule, we think that children aged 13 and above are capable of making a subject access request on their own behalf, but whether this is possible will depend upon the ability and maturity of the child in question. A child who is capable of making a subject access request can also ask someone to act on his or her behalf in the same way that that an adult can.

For children who are not of sufficient age, maturity or ability to make a request, and for such children only, a person with parental responsibility can make a subject access request. Such a person can also ask someone else to act on his or her behalf in making a subject access request about a child for whom he or she has parental responsibility. You will need to provide a signed authorisation for this person to act on your behalf.
Please complete this form if you wish to see data about a child for whom you have parental responsibility. You will also need to provide **proof of your identity**. Your request will normally be processed within one month upon receipt of a fully completed form and proof of identity. You must complete sections 1 and 2 for us to process this request. Section 3 must be completed as well if someone is acting on your behalf as the person with parental responsibility

Proof of identity:

We require proof of your identity before we can disclose personal data. Proof of your identity should include a copy of **two documents** such as your birth certificate, passport, driving licence, official letter addressed to you at your address e.g. bank statement, recent utilities bill or council tax bill. The documents should include your name, date of birth and current address. If you have changed your name, please supply relevant documents evidencing the change.

Administration fee:

LBS's policy is not to charge for Subject Access Requests. However, a 'reasonable fee' may be charged when a request is manifestly unfounded or excessive, particularly if it is repetitive. We may also charge a reasonable fee to comply with requests for further copies of the same information based on the administrative cost of providing the information.
If you wish to have the information printed this is at a cost of £10. Please send a cheque payable to 'The Lady Byron School'

Section 1

If you have parental responsibility and are making a request on behalf of a child[2] (the data subject), please fill in the details of the child below and not your own.

Surname / Family Name:
First Name(s) / Forenames:
Date of Child's Birth:
Address: Postcode
Previous Address: Postcode
Daytime Telephone Number(s):

I am enclosing copies of the following documents as proof of the child's identity Birth Certificate ☐ Passport ☐
If neither of these is available please email the LBS at reception@ladybyronschool.co.uk
Personal Information If you only want to know what information is held in specific records please indicate in the box below. Please tell us if you know in which capacity the information is being held. Information may include personal information provided to the LBS including names, addresses and contact details and may include special category data, for example, a person's ethnicity or religious beliefs. Please tell us as much as you can about what information you think we might hold and when we might have collected this information.
Details:

Section 2

Please complete this section of the form with your details as the person with parental responsibility for the child whose information you are seeking.
It is important that you provide evidence of your identity as well as that of the data subject and proof of your right to act on their behalf.

Title:	Mr	☐	Mrs	☐	Ms	☐	Miss	☐	Other	☐	
Surname / Family Name:											

First Name(s) / Forenames:
Date of Birth:
Address: Postcode
Daytime Telephone Number(s):
Why do you believe the subject is not competent enough to request their information themselves? (for parental requests for students over 12 years old. If the parent believes competency please ask the student to complete the appropriate form).

Please provide proof of identity

I am enclosing copies of the following documents as proof of identity Birth Certificate ☐ Driving Licence ☐ Passport ☐ An official letter to my address ☐
If none of these is available please email the LBS at reception@ladybyronschool.co.uk

What is your relationship to the data subject? (e.g. parent, guardian or legal representative)
I am enclosing the following copy as proof of parental responsibility and legal authorisation to act on behalf of the data subject: Parental responsibility agreement ☐ Court order ☐ Child's birth certificate (if not provided above) ☐ Adoption papers ☐ Other (give details)

Authorised person – Declaration (if available): I confirm that I have parental responsibility for the child who is the data subject. I understand that LBS is obliged to confirm proof of identity/authority and it may be necessary to obtain further information in order to comply with this subject access request.
Name:
Signature:
Date:
Warning: a person who unlawfully obtains or attempts to obtain data is guilty of a criminal offence and is liable to prosecution.

I wish to:
Receive the information in electronic format ☐ (some files may be too large to transmit electronically and we may have to supply in CD format)
Receive the information by post* ☐ Collect the information in person ☐

View a copy of the information only ☐ Go through the information with a member of staff ☐

*Please be aware that if you wish us to post the information to you, we will take every care to ensure that it is addressed correctly. However, we cannot be held liable if the information is lost in the post or incorrectly delivered or opened by someone else in your household. Loss or incorrect delivery may cause you embarrassment or harm if the information is 'sensitive'. **If you wish to have the information printed this is at a cost of £10. Please send a cheque payable to 'The Lady Byron School'**

Please send your completed form and proof of identity to:

Proprietor
The Lady Byron School
The Cedars
11 High Street
Fleckney
Leicestershire
LE8 8AJ
reception@ladybyronschool.co.uk

LBS will retain the information provided and only share the information with those it is legally entitled to. The information will only be retained for as long as necessary and in accordance with LBS's retention policy, will be disposed of in a safe and secure manner.

Appendix 3

The Lady Byron School (LBS) subject access request form: Students aged 13 and over

What rights do children have?
Children have the same rights as adults over their personal data. These are set out in Chapter III and VIII of the UK GDPR and are also listed below. For more detailed information about how these rights apply to all data subjects, please refer to our Guide to the UK GDPR. Where these provisions raise child specific issues these are covered below or elsewhere in our pages on Children and the UK GDPR.
All data subjects, including children have the right to:

- be provided with a transparent and clear privacy notice which explains who you are and how their data will be processed. See 'How does the right to be informed apply to children?';
- be given a copy of their personal data;
- have inaccurate personal data rectified and incomplete data completed;
- exercise the right to be forgotten and have personal data erased. See How does the right to erasure apply to children?;
- restrict the processing in specified circumstances;
- data portability;
- object to processing carried out under the lawful bases of public task or legitimate interests, and for the purposes of direct marketing. See What if I want to market children?;
- not be subject to automated individual decision-making, including profiling which produces legal effects concerning him or her or similarly affects him or her; See What if I want to make automated decisions (including profiling) about children?
- complain to the ICO;
- appeal against a decision of the ICO;
- bring legal proceedings against a controller or processor; and
- claim compensation from a controller or processor for any damage suffered as a result of their non-compliance with the UK GDPR.

When may a child exercise these rights on their own behalf?
Children who are of sufficient age, maturity and ability to make a request are treated in the same way as adults. For these children, the child alone has the right to ask for and see their personal data. As a general rule, we think that children aged 13 and above are capable of making a subject access request on their own behalf, but whether this is possible will depend upon the ability and maturity of the child in question. A child who is capable of making a subject access request can also ask someone to act on his or her behalf in the same way that that an adult can.

If you have already decided that a child is competent to provide their own consent then it will usually be reasonable to assume they are also competent to exercise their own data protection rights.

If a child is competent then, just like an adult, they may authorise someone else to act on their behalf. This could be a parent, another adult, or a representative such as a child advocacy service, charity or solicitor.

When may a parent exercise these rights on behalf of their child?
Even if a child is too young to understand the implications of their rights, they are still their rights, rather than anyone else's such as a parent or guardian.
You should therefore only allow parents to exercise these rights on behalf of a child if the child authorises them to do so, when the child does not have sufficient understanding to exercise the rights him or herself, or when it is evident that this is in the best interests of the child.
This applies in all circumstances, including in an online context where the original consent for processing was given by the person with parental responsibility rather than the child.

How does this work in practice?
An adult with parental responsibility may seek to exercise any of the child's rights on their behalf.

If you are satisfied that the child is not competent, and that the person who has approached you holds parental responsibility for the child, then it is usually appropriate to let the holder of parental responsibility exercise the child's rights on their behalf. The exception to this is if, in the specific circumstances of the case, you have evidence that this is not in the best interests of the child.

If you are confident that the child can understand their rights, then you should usually respond directly to the child. You may, however, allow the parent to exercise the child's rights on their behalf if the child authorises this, or again if it is evident that this is in the best interests of the child.

What matters is whether the child is able to understand and deal with the implications of exercising their rights. So for example, does the child understand what it means to request a copy of their data and how to interpret the information they receive as a result of doing so? When considering borderline cases, you should take into account, among other things:

- where possible, the child's level of maturity and their ability to make decisions like this;
- the nature of the personal data;
- any court orders relating to parental access or responsibility that may apply;
- any duty of confidence owed to the child or young person;
- any consequences of allowing those with parental responsibility access to exercise the child's rights. This is particularly important if there have been allegations of abuse or ill treatment;
- any detriment to the child or young person if individuals with parental responsibility cannot access this information; and
- any views the child or young person has on whether their parents should have access to information about them.

Please fill in your personal details below

Surname / Family Name:
First Name(s) / Forenames:
Date of Child's Birth:
Address: Postcode
Previous Address: Postcode
Daytime Telephone Number(s):

I am enclosing copies of the following documents as proof of my identity Birth Certificate ☐ Passport ☐
If none of these is available please email the LBS at reception@ladybyronschool.co.uk
Personal Information If you only want to know what information is held in specific records, please indicate in the box below. Please tell us if you know in which capacity the information is being held. Information may include personal information provided to the LBS including names, addresses and contact details and may include special category data, for example, a person's ethnicity or religious beliefs. Please tell us as much as you can about what information you think we might hold and when we might have collected this information.
Details:

Declaration : I confirm that I am the child who is the data subject. I confirm that I am fully aware and understand the implications of receiving my data records held by LBS. I understand that I am within my rights not to share any of the information received with any other person and that LBS will send the information directly to me. I am responsible for keeping this data confidential, once received. I understand that LBS is obliged to confirm proof of identity/authority and it may be necessary to obtain further information in order to comply with this subject access request.

Name:
Signature:
Date:
Warning: a person who unlawfully obtains or attempts to obtain data is guilty of a criminal offence and is liable to prosecution.

I wish to:

Receive the information in electronic format ☐ (some files may be too large to transmit electronically and we may have to supply in CD format)

Receive the information by post* ☐ Collect the information in person ☐

View a copy of the information only ☐ Go through the information with a member of staff ☐

*Please be aware that if you wish us to post the information to you, we will take every care to ensure that it is addressed correctly. However, we cannot be held liable if the information is lost in the post or incorrectly delivered or opened by someone else in your household. Loss or incorrect delivery may cause you embarrassment or harm if the information is 'sensitive'.

If you wish to have the information printed this is at a cost of £10. Please send a cheque payable to 'The Lady Byron School'

Please send your completed form and proof of identity to:

Proprietor
The Lady Byron School
The Cedars
11 High Street
Fleckney
Leicestershire
LE8 8AJ
reception@ladybyronschool.co.uk

LBS will retain the information provided and only share the information with those it is legally entitled to. The information will only be retained for as long as necessary and in accordance with LBS's retention policy, will be disposed of in a safe and secure manner.