Alderbrook School | Alderbrook Sixth Form

Data Protection Policy

Author	Mr Tom Beveridge
Date	July 20
Version	1
Approved Date	July 2020
Review Date	July 2021

Aims

1 The governors and senior leadership team of Alderbrook School are committed to ensuring that all personal data collected is processed in accordance with all relevant data protection laws including the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA 2018). Alderbrook School is registered as a data controller with the Information Commissioner.

2 The details of Alderbrook School's Data Protection Officer can be found in paragraph 23.

Scope

3 This policy applies to anyone who has access to and/or is a user of school ICT systems, both in and out of the School, including staff, governors, students, volunteers, parents / carers, visitors, contractors, and other community users.

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

Distribution

5 This policy is available on the school website and in hard copy from the School office.

6 In order to comply with the fair processing requirements of the GDPR, the School informs parents / carers of all pupils / students of the data it collects, processes and holds on the pupils / students and staff, the purposes for which the data is held and any third parties to whom it may be passed. This information forms part of the Privacy Notice which is posted on the main School website in the policy section.

7 A paper copy of the Privacy Notice(s) is available on request from the School office. Privacy Notices are reviewed at least annually, and parents and staff will be alerted to any significant changes via email / text.

Definitions

8 **Personal data** - Any combination of data items which could identify a living person and provide specific information about them, their families or circumstances. The term covers both facts and opinions about an individual. The School may process a wide range of personal data of staff (including governors and volunteers), students, their parents or guardians as part of its operation.

9 This personal data may include (but is not limited to):

- names and addresses (including email addresses),
- bank details,
- academic data e.g. class lists, pupil / student progress records, reports, disciplinary actions, admissions and attendance records
- references,
- employment history,
- taxation and national insurance records,
- appraisal records,
- examination scripts and marks

10 **Special category personal data** - Personal data which is more sensitive and so needs more protection, including information about a living 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

11 Criminal records are treated in much the same way as other special category data

12 **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.

13 **Data subject** - The identified or identifiable (living) individual whose personal data is held or processed.

14 **Data controller -** A person or organisation that determines the purposes and the means of processing of personal data.

15 **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.

16 **Personal data breach** - A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

Roles and Responsibilities

17 This policy applies to all staff (including volunteers and governors) who work at the School, and to external organisations or individuals working on its behalf.

18 **Governing Body -** The Governing Body has overall responsibility for ensuring that the School complies with all relevant data protection obligations.

19 **Headteacher -** The Headteacher acts with the delegated authority of the Governing Body on a day to day basis and will liaise with the DPO. In the Headteacher's absence, in case of emergency, this role will be delegated to a member of the Senior Leadership Team.

20 **All staff -** All staff are responsible for:

- Familiarising themselves with and complying with this policy and acceptable use policies for staff. The learning culture within the organisation seeks the avoidance of a blame culture and is key to allowing individuals the confidence to report genuine mistakes. However, staff should be aware, that a deliberate or reckless disregard of this policy could result in disciplinary action being taken;

- Taking care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse at all times. All staff should adopt the approach that they should treat the personal data of others with the same care with which they would treat their own;
- Using personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data;
- Storing, transporting and transferring data using encryption and secure password protected devices;
- Not transferring personal data offsite or to personal devices
- Deleting data in line with this policy and the retention schedule
- Informing the School of any changes to their personal data, such as a change of address
- Reporting to the Headteacher, or in their absence the DPO in the following circumstances:
    - Any questions about the operation of this policy, data protection law, retaining or sharing personal data or keeping personal data secure;
    - If they have any concerns that this policy is not being followed;
    - If they are unsure whether they have a lawful basis upon which to use personal data in a particular way;
    - If they need to rely on or capture consent, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area;
    - The discovery of a data breach or near miss (immediate action is required) – please refer to the Data Breach Policy and paragraphs 45 – 47 of this policy.
    - Whenever they are engaging in a new activity that may affect the privacy rights of individuals;
    - If they are to share personal data with a data processor, for example a contractor or someone offering a service, in which case a contract is likely to be required please see - *Sharing Personal Data* (paragraphs 40 – 41)

Data Protection Officer (DPO)

21 The Data Protection Officer (DPO) is responsible for advising on the implementation of this policy, monitoring compliance with data protection law, providing support and developing related policies and guidelines where applicable, in amongst other data protection related functions. They will provide an annual report on compliance directly to the governing body and, where relevant, provide the School with advice and recommendations on data protection issues.

22 The School has appointed i-West as its DPO and they can be contacted by email at

Email: i-west@bathnes.gov.uk.

Telephone: 01225 395959

One West

Bath and North East Somerset Council

Guildhall

High Street

Bath

BA1 5AW

23 Under usual circumstances the Headteacher or a member of SLT will be the point of contact with the DPO.

Subject Access Requests and Other Rights of Individuals

24 In all aspects of its work, the School will ensure that the rights of the data subject are protected by all practicable measures associated with the conduct of the School's work. Subject to exceptions, the rights of the data subject as defined in law are;

The Right to be informed.

25 The School advises individuals how it will use their data through the use of transparent Privacy Notices and other documentation such as consent forms where appropriate.

The Right of access

26 An individual when making a subject access request (SAR) is entitled to the following;

- confirmation that their data is being processed;
- access to their personal data;
- other supplementary information – this largely corresponds to the information that should be provided in a Privacy Notice.

27 The School must respond to such a request within 30 days unless the request is complex, in which case it may be extended by a further 60 days. Please refer to Appendix 1 for further details as to how to manage a subject access request.

The Right to rectification

28 Individuals have the right to ask to rectify information that they think is inaccurate or incomplete. The School has a duty to investigate any such claims and rectify the information where appropriate within 30 days, unless an extension of up to a further 60 days can be justified.

The Right to erasure

29 The right for an individual to request that their data is erased is not absolute. It applies where:

- the information was given voluntarily, consent is now withdrawn and no other legal basis for retaining the information applies;
- the information is no longer required by the School;
- a legal obligation to erase the data applies;
- the data was collected from a child for an online service;
- the School has processed the data on the basis that it is in their legitimate business interests to do so, and having conducted a legitimate interests test, it concludes that the rights of the individual to have the data erased outweigh those of the School to continue to process it.

The Right to restrict processing

30 An individual may ask the School to temporarily limit the use of their data when it is considering:

- a challenge made to the accuracy of their data, or
- an objection to the use of their data.

31 In addition, the School may be asked to limit the use of data rather than delete it , if the individual does not want the School to delete the data but does not wish it to continue to use it, in the event that the data was processed without a lawful basis or to create, exercise or defend legal claims.- .

The Right to data portability

32 An individual can make a request in relation to data which is held electronically for it to be transferred to another organisation or to themselves where they have provided it either directly or through monitoring activities e.g. apps. The School only has to provide the information where electronically feasible.

The Right to object

33 Individuals have a right to object in relation to the processing of data for

- a task carried out in the public interest
- a task carried out in its legitimate interests
- scientific or historical research, or statistical purposes, or
- direct marketing.

The Right to withdraw consent to processing

34 Individuals have the right to withdraw their consent to the processing of their data.

Rights related to automated decision making

35 This does not apply as the School does not employ automated decision making processes.

Data Protection Principles

36 The GDPR is based on 7 key data protection principles that the School complies with.

37 The principles say that personal data must be:

- **Processed lawfully, fairly and in a transparent manner** – the School will explain to individuals why the School needs their data and why it is processing it – for example on consent forms (where consent is used as the basis for processing), and in its Privacy Notice(s). The School reviews its documentation and the basis for processing data on a regular basis.
- **Collected for specified, explicit and legitimate purposes** – the School explains these reasons to the individuals concerned when it first collects their data. If the School wishes to use personal data for reasons other than those given when the data was first obtained, it will inform the individuals concerned before doing so, and will seek consent where necessary and appropriate unless the new purpose is compatible with that in respect of which consent was given, or there is another lawful basis for sharing the

information/ The School will document the basis for processing. For special categories of personal data, it will also meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018.

- **Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed -** the School must only process the minimum amount of personal data that is necessary in order to undertake its work.
- **Accurate and, where necessary, kept up to date** – the School will check the details of those on its databases at appropriate intervals and maintain the databases. It will consider and respond to requests for inaccurate data to be rectified in accordance with the Data Protection Act 2018.
- **Kept for no longer than is necessary for the purposes for which it is processed** – when the School no longer needs the personal data it holds, it will ensure that it is deleted or anonymised in accordance with the retention schedule.
- **Processed in a way that ensures it is appropriately secure** – the School implements appropriate technical measures to ensure the security of data and systems for staff and all users and ensure that these are processed in a manner that ensures appropriate security of the personal data, including protection against accidental loss, destruction or damage, using appropriate technical measure.
- **Accountability –** The School complies with its obligations under data protection laws including the GDPR and can demonstrate this via the measures set out in this policy, including:

    - Completing Data Protection Impact Assessments (DPIAs) where the School's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies. This largely involves special category personal data and CCTV. However, the School will liaise with the DPO who will advise on this process. Any activity involving the processing of personal data must be registered on the Register of Processing Activity and reviewed, at the very least, annually;
    - 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; the School also maintains a record of attendance;
    - Regularly conducting reviews and audits to test its privacy measures and ensure compliance with relevant legislation and school policies;
    - Maintaining records of its processing activities for all personal data that it holds.

Processing Personal Data

38 In order to ensure that the School's processing of personal data is lawful; it will always identify one of the following six grounds for processing **before** starting the processing:

- 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 where necessary, balancing the rights of freedoms of the individual). However, where the School can use the public task basis for processing, it will do so rather than rely on legitimate interests as the basis for processing.
- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear consent. In the case of **special categories of personal data**, this must be **explicit consent.** The School will seek consent to process data from the pupil or parent depending on their age and capacity to understand what is being asked for.

39 For processing special categories of personal data an additional lawful basis is needed – these are detailed in theData retention policy .

Sharing Personal Data

40 Please refer to the School's Privacy Notices.

41 The School will only share personal data under limited circumstances, when there is a lawful basis to do so and where identified in the Privacy Notice(s). The following principles apply:

- The School will share data if there is an issue with a pupil or parent/carer that puts the safety of staff at risk;
- The School will share data where there is a need to liaise with other agencies. It will seek consent as necessary and appropriate before doing so. However, where child protection and safeguarding concerns apply, it will apply the "Seven golden rules of information sharing" which provide that in limited circumstances data may be shared with external agencies without the knowledge or consent of the parent or child;
- The School's suppliers and contractors need data to provide services – for example, IT companies. When sharing data the School will:
    - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law;
    - Establish a data processing contract 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 it shares where there is regular sharing;
    - Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with the School.
- The School may also share personal data with law enforcement and government bodies where there is a lawful requirement / basis for us to do so, including:
    - For the prevention or detection of crime and/or fraud;
    - For the apprehension or prosecution of offenders;
    - For the assessment or collection of tax owed to HMRC;
    - In connection with legal proceedings;
    - For research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided.

- The School may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects pupils or staff.

Data Protection by Design and Default

42 The School has a legal obligation to integrate appropriate technical and organisational measures into all of its processing activities, and to consider this aspect before embarking on any new type of processing activity.

43 It is a statutory requirement that any activity involving a high risk to the data protection rights of the individual when processing personal data be assessed by the Data Protection Impact Assessment. Prior to the assumption of any such activity i-west must be consulted and an initial screening be conducted assessing risk.

Personal data breaches or near misses

44 A personal data breach is defined as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a public electronic communications service." It may be deliberate or accidental.

45 Wherever it is believed that a security incident has occurred or a 'near miss' has occurred, the staff member must inform the Headteacher and DPO **immediately** in order that an assessment can be made as to whether the Information Commissioner's Office (ICO) should be informed within 72 hours as is legally required, and / or those data subjects affected by the breach. The learning culture within the organisation seeks the avoidance of a blame culture and is key to allowing individuals the confidence to report genuine mistakes.

46 Further details on security incidents and data breaches can be found in the Data Breach Policy.

Biometric Recognition Systems

47 Biometric data consists of personal information about an individual's physical or behavioural characteristics which may be used to identify that person. It may take the form of fingerprint, voice or facial recognition. We use biometric fingerprinting for our cashless catering system.

48 We will undertake a data protection impact assessment before implementing any new system to assess the impact on individuals

49 In accordance with the Protection of Freedoms Act 2012, once satisfied, we will notify all those with parental responsibility in the case of any student under 18, unless this is impractical (for example the whereabouts of the parent is unknown or if there is a safeguarding issue) and may only proceed if we have at least one positive written consent, and no written parental objection. We will not proceed to process the information if the student themselves objects. Either parents or the student may withdraw their consent at any time, although parents must object in writing.

50 In the case of adults, for example staff members, we will seek their consent direct from them before processing any biometric data.

51 If the individual concerned does not agree to proceed or wishes to withdraw their consent to the use of the biometric system, we will provide an alternative means of achieving the same aim.

Destruction of records

52 We apply our retention policy and will permanently destroy both paper and electronic records securely in accordance with these timeframes.

53 We will securely destroy hard copies and will ensure that any third party who is employed to perform this function will have the necessary accreditations and safeguards.

54 If we delete electronic records and our intention is to put them beyond use, although it may be technically possible to retrieve them, we follow the Information Commissioner's Code of Practice on deleting data and this information will not be made available on receipt of a subject access request.

Training

55 To meet our obligations under Data Protection legislation, we ensure that all staff, volunteers, and governors receive an appropriate level of data protection training as part of their induction. Those who have a need for additional training will be provided with it, for example relating to use of systems or as appropriate.

56 Data protection also forms part of continuing professional development, and updates will be provided where changes to legislation, guidance or the School's processes make it necessary.

Monitoring Arrangements

57 Whilst the DPO is responsible for advising on the implementation of this policy and monitoring the School's overall compliance with data protection law, the School is responsible for the day to day implementation of the policy and for making the data protection officer aware of relevant issues which may affect the School's ability to comply with this policy and the legislation.

58 This policy will be reviewed annually, unless an incident or change to regulations dictates an earlier review.

Complaints

59 The School is always seeking to implement best practice and strives for the highest standards. The School operates an "open door" policy to discuss any concerns about the implementation of this policy or related issues. The School's complaints policy may be found on its website.

60 You have a right to make a complaint to the Information Commissioner's Office (ICO), but under most circumstances the ICO would encourage the complainant to raise the issues in the first instance with the School (201office@alderbrook.solihull.sch.uk) or via the School's DPO.

61 The ICO is contactable at;

Wycliffe House,

Water Lane,

Wilmslow,

Cheshire,

SK9 5AF.

Telephone: 0303 123 1113.

Legislation and Guidance

62 This policy takes into account the following:

- The General Data Protection Regulation (GDPR) 2016
- The Data Protection Act (DPA) 2018.
- The Protection of Freedoms Act 2012
- Guidance published by the Information Commissioner's Office
- Protection of biometric information of children in schools and colleges – DFE March 2018

Links with Other Policies

63 This Data Protection Policy is linked to the following:

- Data Breach Policy
- Safeguarding Policy
- E-Safety Policy

Appendix 1 – Subject Access Request Procedure (SAR)

The school shall complete the following steps when processing a request for personal data (Subject Access Request or SAR) with advice from its Data Protection Officer (i-west).

1. Ascertain whether the requester has a right to access the information and capacity.

2. Obtain proof of identity (once this step has been completed the clock can start)

3. Engage with the requester if the request is too broad or needs clarifying

4. Make a judgement on whether the request is complex and therefore can be extended by an additional 2 months

5. Acknowledge the requester providing them with

   a) the response time – 1 month (as standard), an additional 2 months if complex; and

   b) details of any costs – Free for standard requests, or you can charge, or refuse to process if the request is manifestly unfounded or excessive, or further copies of the same information is required, the fee must be in line with the administrative cost

6. Use its Record of Processing Activities and/or data map to identify data sources and where they are held

7. Collect the data (the organisation may use its IT support to pull together data sources – for access to emails the organisation can do so as long as it has told staff it will do so in its policies)

8. If (6) identifies third parties who process it, then engage with them to release the data to the school.

9. Review the identified data for exemptions and redactions in line with the ICO's Code of Practice on Subject Access and in consultation with the organisation's Data Protection Officer (i-west).

10. Create the final bundle and check to ensure all redactions have been applied

11. Submit the final bundle to the requester in a secure manner and in the format they have requested.