DATA PROTECTION AND CONFIDENTIALITY POLICY

Status	Statutory	Date created	22 May 2018
Any other statutory names for this policy (where applicable)		Date last reviewed	Approved by Governors Summer 2025
Responsibility for this policy (job title)	Deputy Headteacher	Frequency of review	Annually
Governors' Committee with responsibility for its review and monitoring	Personnel Sub Committee	To be put on the school website? (Yes/No)	Yes
Approval : Sub committee			

Introduction

1. Under the Data Protection Act 2018 and the General Data Protection Regulations (GDPR), the school must follow certain rules regarding the storing and using of data relating to individuals. This policy sets out how the school meets the requirements of the Act.

2. This policy applies to all staff at AHS. The term "staff" includes paid employees, Governors and other persons, whether under contract or not, who are granted access to data of a personal nature in order to carry out their duties at AHS. Examples of other persons include volunteers, student teachers, contractors, coaches, peripatetic music tutors. *It is the responsibility of relevant departmental heads to ensure unpaid staff working in their area are aware of the provisions of this Policy.*

3. Since data protection is a critical issue for the School, any breach of this policy may result in disciplinary action for the individual. It could also result in a fine or possible prosecution against either the school or the individual.

4. It is, therefore, the responsibility of all staff to ensure they are acquainted with the principles of this policy and that they abide by its detail. Any member of staff not entirely sure of how to handle data of a personal or sensitive nature should seek advice from a departmental head, Data Protection Lead or member of the Senior Leadership Team.

5. Confidentiality: Although the Act is primarily aimed at the organisation level, all staff have a duty to maintain appropriate levels of confidentiality internally, as well as protecting data from outside loss or disclosure. Therefore, this Policy also deals with the principles and procedures to maintain internal confidentiality. Maintaining a correct approach to confidentiality at all levels:

    - builds trust between parents/carers, students, staff and visiting professionals
    - supports the education and welfare of students by empowering them to talk to adults within school in a safe and supportive environment
    - prevents the need to deal with each disclosure as a crisis in isolation
    - removes uncertainty and inconsistency in how different disclosures of information are handled
    - allows the school's management to provide support to staff whilst ensuring they can work in an environment free of gossip and social pressure

Data Protection Lead and Officer

6. The IT manager acts as the Data Protection Lead (DPL) and the Deputy Headteacher (Curriculum) is the Data Protection Officer (DPO).

7. Their role is to oversee and monitor the school's data protection procedures and to ensure they are compliant with the GDPR. In broad terms the role is split as follows:

    - The DPL will inform and advise the school and its employees about their obligations to comply with the GDPR and other data protection laws, including internal data protection activities, advising on data protection impact assessments.

    - The DPO will monitor compliance with the GDPR and other data protection laws, conduct internal audits, investigate any data breaches and arrange for staff training. The DPO will produce an annual report for the governing body.

General Principles

8. The GDPR requires that under the following principles data is:

    - used fairly and lawfully and in a transparent manner
    - only collected for specified, explicit and legitimate purposes
    - not used beyond the specified purposes or in a manner incompatible with those purposes
    - adequate, relevant and limited to what is necessary for those purposes
    - accurate and, where necessary, kept up to date
    - kept in a form which permits identification of data subjects for no longer than necessary
    - processed in a manner that ensures appropriate security of personal data.

9. In general this means that the school should:

    - only hold data that it requires to fulfil its function and not hold other data unnecessarily
    - only hold data with the knowledge of the individual affected and make that data easily available to the individual within the limits of the law
    - only hold and use data in a manner that complies with the law
    - safeguard data to prevent it being available to unauthorised bodies or misused

- maintain systems to ensure data which is no longer required is securely deleted or otherwise destroyed.

Definitions of Data and Confidential information

10. Personal data: The GDPR applies to 'personal data' meaning any information relating to a person who can be directly or indirectly identified by reference to the data or combinations of data. This includes name, identification number, address and contact information (including email address), student assessment data (e.g. mark books and exam results) as well as more sensitive linked data such as biometric data (including identifiable photographs) or medical information.

11. Sensitive personal data: The GDPR refers to sensitive personal data as 'special category data' and this is defined as:

    a. personal data revealing racial or ethnic origin;
    b. personal data revealing political opinions;
    c. personal data revealing religious or philosophical beliefs;
    d. personal data revealing trade union membership;
    e. genetic data;
    f. biometric data (where used for identification purposes);
    g. data concerning health;
    h. data concerning a person's sex life; and
    i. data concerning a person's sexual orientation.

    Special category data is more likely to cause more personal harm if not protected and so needs more protection.

12. Confidential information: Confidential information is personal data or information which is shared with someone on the understanding that it can only be passed on to a third party with the agreement of the person disclosing it (apart from where there is a legal duty to share). There is other non-personal confidential information, e.g. commercial contract prices, which does not fall under the act or this policy but will demand the appropriate level of protection.

Specific Requirements

13. Lawful Basis: The School is required to have a valid Lawful Basis for any processing of personal data. The School is required to record the Lawful Basis for processing personal data before it is collected and it does this by maintaining a Data Register on a system called GDPRiS. It is a requirement for all staff to ensure any personal data they collect or use is already recorded in the School's Data Register and if not, take personal responsibility for recording it fully in that Register. There are 6 classes of Lawful Basis and at least one must apply to all personal data collected, retained and processed by the School:

    - **Contract**: the processing is necessary for a contract the school has with the individual, or because they have asked the school to take specific steps before entering into a contract. This will apply to employee data.
    - **Legal obligation**: the processing is necessary for the school to comply with the law (not including contractual obligations). The sort of data this would apply to is data required by the HMRC or a court order, but data the school is obliged by statute to process for the DFE is a Public Task.

- **Vital interests:** the processing is necessary to protect someone's life (who may not be the subject of the data). This may apply to safeguarding or medical information but should not be used if the individual is capable of giving consent, even if they refuse their consent. A likely use of this is where the school needs to use a parent's personal data to protect the vital interests of a child.

- **Public task**: the processing is necessary for the school to perform a task in the public interest or for the school's official functions and the task or function has a clear basis in law. This will apply to most of the routine data dealing with students.

- **Legitimate interests**: the processing is necessary for the school to fulfil its lawful function. This basis would be most appropriate where the school uses people's data in ways those people would reasonably expect and which have a minimal privacy impact. This may also include allowing for the legitimate interests of a third party, for example a staff benefit scheme managed by an external company, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

- **Consent**: For work which does not fall into one of the other categories, personal data may still be collected and used if the individual has given their clear and explicit consent. The GDPR sets a high standard for consent but the school does not always need consent if the data is held and processed under one of the other Lawful Bases. This form of consent should not be confused with parental consent, such as allowing a student to go on a trip. An example of when consent would be appropriate as a Lawful Basis for storing and using personal data is in the area of fundraising. Consent means offering individuals real choice and control and should put individuals in charge, build trust and engagement and enhance the school's reputation. If consent is the Lawful Basis then the following provisions must also be met:

    a. there must be a positive opt-in; there cannot be pre-ticked boxes or any other method of default consent
    b. there must be a very clear and specific statement of consent at the point that it is given13
    c. consent requests must be separate from other terms and conditions
    d. consent must be specific, clear, concise and 'granular' (ie the school must get separate consent for separate things)
    e. any third parties who will rely on the consent must be identified
    f. it must be easy for people to withdraw consent and the school should tell them how
    g. the school must keep evidence of consent – who, when, how, and what people were told
    h. provisions under the basis consent should be reviewed annually and updated as required
    i. unless absolutely necessary, consent to processing should not be a precondition of a service
    j. where consent is the Lawful Basis and the data subject is a student, they should be 13 years or older to give their consent; otherwise the parent must provide consent.

14. Students' rights to confidentiality: There is no statutory requirement for schools to always inform parents/carers of confidential disclosures made by students. Disclosures will be dealt with on a case by case basis and advice will be sought from agencies, such as School Health, First Response (Social Care) or the Safeguarding in Education

team, where a difficult judgement has to be made. The student's welfare will be paramount in any decisions made surrounding information sharing. *Where the student withholds their permission to inform their parent, staff should consider if the student is able to make that decision*[1]. Likely exceptions where there can be no right to confidentiality include:

- where there is a risk of serious harm or threat to life
- where the information forms or might form part of a Child Protection case which comes under section 47 of the Children Act (1989)
- where a student needs urgent medical treatment
- where potential or actual serious crime (e.g. assault) is involved
- where safeguarding national security is involved (e.g. terrorism)

15. Special Category Data: In order to lawfully process special category data, the school must identify both a Lawful Basis and a separate condition for processing special category data. There are ten conditions for processing special category data in the GDPR and the school must determine, and document, the applicable condition before the data is collected or used and before it begins this processing under the GDPR. The conditions which may apply to the school are:

    - the data subject has given explicit consent to the processing of their personal data for one or more specified purposes
    - the data is required to meet obligations in the field of employment and social security and social protection law
    - processing is necessary to protect the vital interests of the data subject or of another person who is physically or legally incapable of giving consent
    - processing relates to personal data which is manifestly made public by the data subject
    - processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity
    - processing is necessary for reasons of substantial public interest
    - processing is necessary for the purposes of occupational medicine for the assessment of the working capacity of the employee.

16. Criminal Conviction Data: The processing of data relating to criminal convictions is treated in a similar way to special category data but requires both a legal basis and official authority. Within the school context this is limited to the Disclosure and Barring System for staff.

17. Individuals' Rights: Individuals have the following rights:

    - the right to be informed[2]
    - the right of access
    - the right to rectification

[1] Commonly known as the Fraser Guidelines, following the case of Victoria Gillick 1985, the judge gave the following advice: "It is suggested that a child or young person's ability to make decisions about his/her life depends on him/her having "sufficient understanding and intelligence to be capable of making up his/her own mind".

[2] The school primarily meets the right to be informed through the publication of privacy notices (see Annex C).

- the right to erasure
- the right to restrict processing
- the right to data portability
- the right to object
- rights in relation to automated decision making and profiling.

18. Enquiries: The focal point for enquiries relating to student, parent or staff data and the Data Protection Policy is the Data Protection Lead. Requests by the individual to access their full data should be processed in accordance with the Subject Access Request procedure in Annex A. Updates to data, such as change of address, are routinely made by the Data Team (for staff or students) or Pastoral Support Assistants (for students only). Any enquiries by an individual about their personal data should, in the first instance, be passed to the relevant person listed here. If there is uncertainty as to how the request should be handled, it can be referred to the DPL.

19. Disclosures to Staff by Staff, Students or Parents: *Where staff, students or parents wish to talk to school staff about confidential matters they should be advised (wherever possible, prior to a disclosure) what kinds of disclosure will require information to be shared, what will be done with the information and who else will have access to it.* This will be routinely included at the start of lessons, such as some L4L lessons, where disclosures are more likely. After the disclosure, the disclosing person will be consulted on how and with whom any information will be shared[3]. If a member of staff is unsure of how to proceed when faced with a disclosure, they must discuss the case (without disclosing the person's identity in the first instance) with a senior member of staff (if relating to a student this should be the Designated Safeguarding Lead (DSL) or a member of the DSL Team).

20. Sharing of confidential information between staff: Confidential information about parents, students or other members of staff will only be shared with colleagues on a 'need to know' basis with the disclosing party having given prior agreement for the information to be shared, unless exempted by legislation. *Discussions involving confidential information need to take place in a confidential environment;* public places such as the staffroom, the classroom and corridors are not, in general, confidential environments.

21. Registration: The school is registered with the Information Commissioner's Office (ICO) under Registration Number Z2665284.

22. Documentation: The GDPR requires the School to document its data processing activities. This is achieved by using Records of Processing Activities that are stored on a system called GDPRiS. *Before collecting or using any personal data about employees, students or parents, it is a responsibility of the member of staff intending to use the data that the record is checked to ensure the type of data and the use to which it will be put are properly documented.* In the event that it is not, the DPL must be informed so that they can record the activity and ensure that there is a lawful basis for processing the data.

23. Contracts with outside agencies: It is a requirement that whenever the school uses a third party to process personal data there needs to be specific GDPR-compliant clauses in the contract. *No staff are to enter into a contract with a third party which involves the transfer of personal data without first seeking the advice of the DPL.* Where there is no formal contract but data will be passed to a third party (e.g. in dealing

[3] See the Safeguarding and Child Protection Policy

with safeguarding issues), the external parties are to be made aware of the school's Data Protection and Confidentiality Policy.

24. Limited Use: *Staff must only use data held by the school for a purpose linked to their role within the school*. Data must never be used for a personal reason unless the express permission has been obtained from the individual or parent[4] as appropriate.

25. Adequate but not Excessive: Data which the school does not need to hold for either its own purposes or for statutory reporting requirements should not be recorded. Some important personal data is needed for specific short term events and this information must be deleted or disposed of once the event has come to a conclusion and no later than 12 months after the event. For example, student passport information is not required for the functioning of the school and so should not be routinely recorded but would be needed for an overseas school trip.

26. Accuracy: *It is the responsibility of all staff to notify the relevant department if they discover any inaccuracy in data records*. Additionally, staff, parents and students can check their data accuracy and notify us of any changes by accessing Edulink.

27. Challenge to Prejudicial Records: In the event that an individual challenges the accuracy of a record, the nature of which might be prejudicial to the school or the individual, the matter should be referred to the Headmistress who must take a judgement on what is fair to both sides, with the emphasis on fairness to the individual. If the outcome is disputed then reference is to be made to the Complaints Policy.

28. Retention of Data: The time period for which we retain data can be found in our data retention procedure and this can be requested from school if required.

29. Requests for Access to Data: The Data Protection Act extends to all individuals regardless of age and so students, parents and staff have a right of access to their own personal data. If the child is under the age of 12 or a person is deemed to be not capable of making decisions about their data, a parent or carer can make decisions on their behalf. The rights an individual has are as follows:

    a. the right to access personal data held about them (the right of subject access)
    b. the right to be informed about how and why the data is used
    c. the right to have their data rectified, erased or restricted
    d. the right to object
    e. the right to portability of their data
    f. the right not to be subject to a decision based solely on automated processing

    In order to ensure that people receive only information about themselves, requests must be made in writing (an email from an email address registered with the school is acceptable) and on receipt these are to be passed to the relevant focal point. Requests made by an agent, e.g. solicitor, acting on behalf of an individual will only be accepted where there is evidence that the individual has authorised the agent. Where a request for access to personal data is received, the Subject Access Request Procedure (see Annex A) will be followed and the following will apply:

    a. Requests from students who do not appear to understand the nature of the request will be referred to their parents or carers. In general it is accepted

[4] Whenever the term parent is used, it equally applies to someone with parental responsibility.

that a student over the age of 12 should be able to understand the nature of their request and the required information will be given directly to them.

b. Requests in respect of their own child from parents with legal parental responsibility will be processed as requests made on behalf of the student and the information will be sent to the requesting parent. Such requests for students over the age of 12 should only be accepted with the knowledge and agreement of the student, unless it is clear that the student does not understand the implications.

c. There are some circumstances where information may be exempt such as: where the information may cause harm; reveal a risk of abuse; or relate to court proceedings, adoption or parental orders; and there are special rules involving examinations. When appropriate, the school will inform you of the exemption and let you know of the documents where the exemption has been applied.

d. Charges may not be made for copies of records supplied to an individual unless it is a repeated request for the same information; in the latter case the DPL will be able to advise on what would be a reasonable charge.

e. Unless there are extenuating circumstances, written requests for access should be dealt with as soon as possible and no later than within one calendar month of the request. If this timescale is going to prove difficult because the request is difficult, the requestor should be informed immediately with the reasons why it is difficult and a revised date (up to a maximum of 3 months after the request date).

f. Personal data being supplied in response to a request for access must only be supplied to the individual in person, or their verified agent, and once their identity has been verified. The individual should be asked to sign a receipt for the data. This will usually mean the individual should collect the data in person from school unless an alternative, recordable and secure method of transfer can be identified.

30. Biometric Data: The school uses biometric data to make the process of issuing library books and paying for meals simpler, safer and more efficient and for identity verification purposes on site for safeguarding reasons. For student scanned finger data, at least one parent must give positive consent; where that consent is not obtained the student will still be able to access the services but may be required to use alternative identification systems. The school will obtain this permission on the student's entry to the school and will assume consent continues unless notified otherwise. Students over the age of 13 may give consent in their own right. Biometric data is maintained in an encrypted form on servers on site. Scanned finger data is not to be passed on to any other agencies.

31. Images: Occasionally we may take photographs or film students at school for educational purposes, or for staff training. This could include displaying the images on display boards in classrooms or corridors, in school publications, in our prospectus, on our website or our social media feeds. Staff will ensure that the students will be made aware that they may be photographed or filmed, the purpose of the photographs or recordings and given the option not to be included. Any images that are publicly available will not include the students' full names. Images will only be used where consent has been given.

32. CCTV: The school has CCTV in operation. This is managed under the Health and Safety Management System.

33. Transmission of Data to Third Parties: There are many reasons why data is passed to third parties outside the school. Routinely, administrative data is passed to Local Authorities, Government Departments, the school nursing team and other schools in accordance with legislation and these examples are described in the Privacy Notices at Annex C. These and other instances, where there is a lawful basis of Legitimate Interest to transmit data to third parties, must be recorded in the Records of Processing Activities and consideration given as to whether it would be also appropriate to obtain positive consent from the subject.

34. Data and Computer Security: It is essential that all data is held securely and it is a requirement of all staff to do everything they can to protect data of a personal nature. The following procedures must be rigorously adopted:

    - The school's computer system is to be protected by commercial firewalls, data backup systems and anti-virus software which is to be maintained through means of annual support contracts.

    - Access to the school's computer system is to be by password-protected login and permissions levels are to be set appropriate to the level of access required. *Staff must not share their passwords.*

    - *Staff must not email personal data, other than names and email addresses, to a recipient outside the school's domain unless it has been encrypted.* As a minimum, the Microsoft encryption tools embedded in Word, Excel, etc. are acceptable but not for Special Category data. Passwords relating to this encryption should be transmitted by separate email or by telephone. Any internal emails dealing with sensitive information should have the word "CONFIDENTIAL" in the subject header and not include any individual identifiers in the subject.

    - *If confidential or sensitive information needs to be sent by post, whether it be hard copy or stored on electronic media, then staff should inform reception to use Royal Mail Special Delivery Guaranteed or a trusted courier with a tracking service.* The information should be in a sealed envelope marked on the outside with the word "CONFIDENTIAL" and placed in a second envelope for addressing. The outer envelope should not identify that the contents are sensitive, other than by using "For the personal attention of" or similar. An exception will be made if students ask us to send their exam results home in August; their consent for this would be given by providing us with a stamped addressed envelope or making a payment for the postage on ParentMail.

    - USB drives may not be used for school data. There are limited exceptions such as adhering to requirements set by exam boards. These exceptions will need to be approved by both DPO and CFOO. Where exceptions have been made, personal data on USB drives, CDs and other removable media is not to be taken off the school site unless it has been encrypted and password protection applied. *Staff are personally responsible for ensuring data in their care is suitably encrypted* and help will be provided by the ICT support team.

    - School laptops, netbooks and similar devices are protected by a network login and so are suitable for holding data of a general personal nature such as student reports, dates of birth etc. However, files containing data of a very sensitive

nature, for example which may cause harm if released, should be individually password protected if stored on anything other than the school's internal network.

- Documents and removable media containing data of a sensitive or personal nature are to be secured in locked cupboards overnight and offices are to be secured by keypad or locking when the office is unattended.

  Note: The school uses Google Workspace for Education and the Department for Education has confirmed that this system meets data protection requirements. Staff can use this system to store data, which requires access from off-site. Staff should use hyperlinks in emails in preference to attaching files when sending data to other school staff in order to reduce the chance of data being stolen, intercepted or accidentally deleted. However, staff should not use Google for information of a very sensitive nature, such as child protection information, and should seek advice from the DSL Team.

35. Artificial intelligence (AI): AI tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Gemini. AHS recognises that AI has many uses to help pupils learn, but also poses risks to sensitive and personal data. To ensure that personal and sensitive data remains secure, staff are trained in the use of AI and Gemini is only available to staff through the AHS login. If personal and/or sensitive data is entered into a generative AI tool, AHS will treat this as a data breach, and will follow the personal data breach procedure outlined in Annex B.

36. Data Breaches: A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable and this unavailability has a significant negative effect on individuals. It is a requirement of GDPR that certain types of personal data breach must be reported to the ICO within 72 hours of their occurrence or discovery. *Any member of staff becoming aware of any loss of personal data or erroneous or inappropriate disclosure of personal data must report the matter immediately using the data breach form.* See Annex B for the Data Breach Procedure.

37. Implementation: The Headmistress should ensure that staff are aware of the School's Data Protection Policy and its requirements including procedures. This should be undertaken as part of induction, supervision and ongoing training. If staff have any queries in relation to the school's Data Protection Policy and associated procedures, they should discuss this with their line manager, DPO, DPL or the Headmistress.

Annex A

Subject Access Request Procedure

Subject Access Request (SAR)
If you only want information about a specific incident, you may find that you can get that information by asking for it directly from the department holding it, without having to go through the SAR procedure. It is possible that the department may have to check whether the data can be released, but that shouldn't take too long. If the department is happy to release your data to you in this way, it will be a much shorter and less formal process than the SAR process. However, if you want information from a number of areas of the school the best way is still to use the SAR.

Making a SAR request
All SARs must be made in writing to the school. If a parent is requesting this for a student over the age of 12, the student must also agree to the request. The school provides a form for such requests that is designed to collect the information needed to identify the data you are requesting. If you would like to submit the request using this form, please request the form from the Data Protection Lead and then complete it and send it, with the appropriate identification documents, either by post to the Data Protection Lead, Aylesbury High School, Walton Road, Bucks. HP21 7SX, or by email to DPL@ahs.bucks.sch.uk. If you would prefer, you can bring original identification documents to reception in person. The school does not charge for this service.

Information required for a search
In order to find the data you are requesting, we will need the following information:

Your:

- name
- address
- date of birth
- details of identification provided to confirm name of data subject
- details of the data requested

Identification is required to confirm that you are the data subject – that is, the individual to whom the data refers – so that the school does not disclose any data to someone who is not entitled to receive it.

If you are making a request on behalf of the data subject e.g. you are a solicitor acting on your client's behalf, you will need to provide the information detailed above for the data subject, plus proof that you have your client's consent to request and receive their personal data. This may be a signed form of authority from the individual. It would be helpful to provide some contextual information about the required data e.g. dates that the information may have been produced, or whether it refers to your time as a student or a member of staff.

Types of search
The vast majority of searches for personal data carried out by the school are general searches in relation to students or members of staff. If you are, or were, a student or parent, the school will routinely search the following areas for your data, as these are the areas where most student data is held:

- Paper based student files

- SIMS
- Financial Services
- Oliver (School Library)
- School Matron
- Alumni and Fundraising/Grant Donors

If you would like other areas of the school searched for your data, you can indicate these on the SAR form or in your written request.

If you are, or were, a member of staff, the school will routinely search the following areas for your data, as this is where the majority of staff data is held:

- HR – for your central file containing details of your initial application, any subsequent applications within the school, job changes
- Finance Office – payroll data, payments details, pension details

If you would like other areas searched for your data, you can indicate these department(s) on the SAR form or in your written request.

You may however, only want to receive information relating to a specific incident or issue. If that is the case, please provide as much detail as possible regarding the information you require e.g. dates of events, when the information may have been recorded or where you think the information may be held, to help identify the data you require.

Duration of process
The school has one month in which to provide the data you have requested. This period starts on the date that the school receives all of the information it needs to confirm firstly, your identity, or your right to request a third party's data, and secondly, the type of search you want carried out (either a general search or a search for specific information). The date on which you will receive your requested information will be confirmed once the school has received all the required information. How will your data be provided to you? The General Data Protection Regulation requires that you receive a permanent copy of any personal data held about you. Therefore, you will receive either an electronic or paper copy of the personal data found about you, depending on the preference you selected on the SAR form or in your written request, and the size of the data.

If you wish to receive your data in paper form, this will be sent to you using first class recorded delivery post. The school uses recorded delivery post to ensure an audit trail exists to show where the information was sent, who signed for it and when. In the event that no-one is available to sign for your correspondence from us, it will be held at a local office until it is collected or finally returned to the school. This ensures your data is held as securely as possible until you receive it. If you wish to receive your data electronically, assuming the file size is not too large, it will be sent to you by email as an attachment. The file will be password protected and once you receive the file, you will need to contact the school for the password in order to access the attachment. Information on how to do this will be included in the email that sends your data to you.

Data Provided
You will receive copies of the personal data relating to you. Personal data is defined as data that identifies a living individual and relates to that individual. Therefore, the data you receive will not only name you but also have some reference to you. As the school still holds some paper files as well as electronic records, a search will be carried out initially for files / folders that are named using your name in any format. After that, electronic searches will be carried out for any electronic records that contain your name

in the body of the data – not just the title. It is not always possible to carry out this search fully without any background information on the type of record you are looking for.

Whether you receive copies of particular emails will depend on whether the data may relate to you. So, for example, you will not receive copies of emails that have been sent to a list of email addresses including yours, where the information in the email does not relate to you, eg it is a reminder of a student and graduate employment fair open to everyone. However, you will receive a copy of an email that has been sent to a list of email addresses including yours, where the information in the email does relate to you.

Your personal data may be held in a document or database that contains personal data relating to other individuals. To avoid providing you with a third party's personal data, it may be necessary to redact the other person's data (that is, blank it out or obscure it in other ways) or to extract your data from the larger document / database. Therefore, you may receive copies of documents with blank spaces in the text, or with only one line of information under column headings. These are examples of redacted documents or where your data has been extracted. We will state the reasons for redactions where appropriate.

Exemptions to data sharing
It is important to note that it is not always possible to know exactly what information is held about an individual when a search is made. It may not always be possible for the school to provide every piece of information about your employment or studies, as there may have been some discussions relating to a final decision made at a meeting or over the telephone, which will not always be recorded. Emails are often seen as an informal method of communication and staff are encouraged to retain emails in line with their subject matter, but that does mean that not all emails will be kept for the same length of time. Therefore, an email in which someone agrees to attend a meeting does not need to be kept for as long as one that includes a decision on a particular subject that has ramifications for others or over a length of time.

There may be times when the school holds personal data about you which it does not/cannot disclose to you. This may be because it is not possible to disclose your personal data without disclosing a third party's data, and either the third party has refused to give consent for their data to be disclosed or the third party's data is awarded a degree of confidentiality which means the data cannot be disclosed.

There are other exemptions in the General Data Protection Regulations which mean that personal data can be withheld. Details and examples of these instances can be found in Chapter 9 of the Information Commissioner's Office, Subject Access Code of Practice. If it is necessary to withhold any data, you will be informed of the reasons for the non-disclosure, but the school endeavours to release as much of your data as possible.

Examples of information which (depending on the circumstances) may be withheld includes information that:

- might cause serious harm to the physical or mental health of the student or another individual
- would reveal that the young person is at risk of abuse, where disclosure of that information would not be in their best interests
- is contained in adoption and parental order records and
- is legally privileged, including certain information given to a court in proceedings concerning a child
- records the intentions of the school in negotiations with the individual making the SAR

- consists of a confidential reference given by the school (though not currently confidential references received by the school)
- consists of exam or test answers or exam results before the allotted publication time
- is held for purposes of management planning (e.g. redundancy planning)
- would prejudice the prevention and detection of crime if disclosed (e.g. in live investigations)
- might cause serious harm or distress in limited social work contexts

Next Steps
You may first contact the school to clarify any queries about the information you have received or to point out any omissions in the data that you expected to receive – although if you are looking for anything particular, it is best to stipulate this in your original request. We will look again at the information held within the school to see if any new information can be sourced with the extra detail provided by you.

If you remain dissatisfied with the response to your request, you may submit a complaint to the Information Commissioner's Office (ICO). More advice on how to do this is available by contacting the ICO on its helpline number of 0303 123 1113.

Annex B - Data Breach Procedure

Introduction
Aylesbury High School holds large amounts of personal and sensitive data. Every care is taken to protect personal data and to avoid a data protection breach. In the event of data being lost or shared inappropriately, it is vital that appropriate action is taken to minimise any associated risk as soon as possible. This procedure applies to all personal and sensitive data held by Aylesbury High School and all school staff, Governors, volunteers and contractors, referred to as 'staff'.

Purpose
This breach procedure sets out the course of action to be followed by any member of staff at Aylesbury High School who becomes aware of a data protection breach in their area of responsibility, and the subsequent follow up action by other staff.

Legal Context
Article 33 of the General Data Protection Regulations: Notification of a personal data breach to the supervisory authority

1. In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the Information Commissioner's Office (ICO), the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.[5] Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.
2. The processor shall notify the controller without undue delay after becoming aware of a personal data breach.
3. The notification referred to in paragraph 1 shall at least:

    a. describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

    b. communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;

    c. describe the likely consequences of the personal data breach;

    d. describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

4. Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

5. The controller shall document any personal data breaches[6], comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article.

[5] Section 1 lays down the parameters for reporting a serious data breach to the ICO; in our context this would be one where there is a risk of personal harm or personal loss or damage.
[6] Section 5 is the requirement on the School to record all data breaches, no matter how severe they are.

Types of Breach

6. Data protection breaches could be caused by a number of factors. A number of examples are shown below:

- Loss or theft of student, staff or governing body data and/ or equipment on which data is stored;
- Inappropriate access controls allowing unauthorised use;
- Equipment Failure;
- Poor data destruction procedures;
- Human Error;
- Cyber-attack;
- Hacking.

Managing a Data Breach

7. In the event that the School identifies or is notified of a personal data breach, the following steps should followed:

a. The person who discovers/receives a report of a breach must inform the Data protection Lead (DPL) or in their absence the Headmistress/Deputy Headteacher. The DPL will at the first opportunity inform the Headmistress. If the breach occurs or is discovered outside normal working hours, this should begin as soon as is practicable.

b. The DPL (or nominated representative) must ascertain whether the breach is still occurring. If so, steps must be taken immediately to minimise the effect of the breach. An example might be to shut down a system, or to alert relevant staff such as the IT technician.

c. If the breach is likely to be reported to the ICO the Headmistress or DPL should inform the DPO and the Chair of Governors as soon as possible. As a registered Data Controller, it is the school's responsibility to take the appropriate action and conduct any investigation.

d. The DPL in consultation with the Headmistress must also consider whether the Police need to be informed. This would be appropriate where illegal activity is known or is believed to have occurred, or where there is a risk that illegal activity might occur in the future. In such instances, advice from the School's legal support should be obtained.

8. The DPL must quickly take appropriate steps to recover any losses and limit the damage. Steps might include:

a. Notifying individuals that might be affected by the breach if it is considered there is an immediate and serious risk to them.

b. Attempting to recover lost equipment.

c. Contacting the relevant Local Authority Departments, so that they are prepared for any enquiries on the incident or for further information (including potentially 'phishing') on the individual or individuals concerned.

d. Consideration should be given to a global email to all school staff. If an inappropriate enquiry is received by staff, they should attempt to obtain the enquirer's name and contact details if possible and confirm that they will ring the individual, making the enquiry, back. Whatever the outcome of the call, it should be reported immediately to the DPL.

e. Recovering data by the use of back-ups.

f. If bank details have been lost or stolen, consider contacting banks directly for advice on preventing fraudulent use.

g. If the data breach includes any entry codes or IT system passwords, then these must be changed immediately and the relevant agencies and members of staff informed.

Investigation

9. In most cases, the next stage would be for breach to be fully investigated by the DPL or, in the case of a significant breach, the DPO. The DPL/DPO should ascertain whose data was involved in the breach, the potential effect on the data subject and what further steps need to be taken to remedy the situation. The investigation should consider:

    - The type of data;
    - Its sensitivity;
    - What protections were in place (e.g. encryption);
    - What has happened to the data;
    - Whether the data could be put to any illegal or inappropriate use;
    - How many people are affected;
    - What type of people have been affected (students, staff members, suppliers etc.) and whether there are wider consequences to the breach.

10. A clear record should be made of the nature of the breach and the actions taken to mitigate it. The investigation should be completed as a matter of urgency due to the requirements to report notifiable personal data breaches to the ICO. A more detailed review of the causes of the breach and recommendations for future improvements can be done once the matter has been resolved.

Notification

11. Some people or organisations may need to be notified as part of the initial containment. However, the decision will normally be made once an initial investigation has taken place. The DPO should, after seeking expert or legal advice, decide whether anyone is notified of the breach. In the case of significant breaches, the ICO must be notified by the DPO or DPL within 72 hours of the breach. Every incident should be considered on a case by case basis.

12. The DPL is responsible for organising the notification of external organisations or individuals. The notification should include a description of how and when the breach occurred and what data was involved. Include details of what the School has already done to mitigate the risks posed by the breach. When notifying individuals, the DPL should give specific and clear advice on what the individual can do to protect themselves and what the School is able to do to help them. Individuals should also be given the opportunity to make a formal complaint if they wish via the School's Complaints Procedure.

Review and Evaluation

13. Once the initial aftermath of the breach is over, the DPL and Headmistress, together with the DPO if involved, should fully review both the causes of the breach and the effectiveness of the response to it. It should be reported to the next available Senior Management Team for discussion. If systemic or ongoing problems are identified, then an action plan must be drawn up to put these right. The Headmistress will need to decide if the breach warrants a disciplinary investigation.

Annex C

Privacy Notices - Privacy Notices can be found on our website