DATA PROTECTION AND CONFIDENTIALITY POLICY

Status	Statutory	Date created	22 May 2018
Any other statutory names for this policy (where applicable)		Date last reviewed	May 2020 (Gov) Dec 2021 HT
Responsibility for this policy (job title)	Data Manager	Frequency of review	Annually HT Every three years (Governors)
Governors' Committee with responsibility for its review and monitoring	Personnel Sub Committee	To be put on the school website? (Yes/No)	Yes
Approval : Headteacher annually, sub committee every three years			

Introduction

1. Under the Data Protection Act 2018, also known as 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 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 school has appointed the Support Staff Director, Mr K Marshall, as the Data Protection Lead (DPL) and Mr C King (the DPL at Aylesbury Grammar School) as 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 and arranging for staff training.
    - The DPO will monitor compliance with the GDPR and other data protection laws, conduct internal audits and investigate any data breaches. 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. <u>Personal data:</u> 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 categories of personal data' and this includes medical data, SEND data and biometric data used to uniquely identify an individual (e.g. thumb prints). 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 the Google Drive. *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 given
    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

[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".

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
- 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 student and parent data is the Data Manager. The focal point for staff data and Data Protection Policy is the Support Staff Director. 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 Headteacher's PA (for Staff) and Pastoral Support Assistants (for students). 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

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

[3] See the Safeguarding and Child Protection Policy

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;* e.g. 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. This registration details, the type of data held and the use to which it 'Search the register' function.

22. Documentation: The GDPR requires the School to document its data processing activities. This is achieved by the Data Register. *Before collecting or using any personal data about employees, students or parents, it is a personal responsibility of the member of staff intending to use the data that the Register 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, an additional entry must be made in the Register and the DPL informed, who will then validate the entry.

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 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, the Personal Support Assistants should arrange for staff and parents to be sent a data sheet from time to time to ensure accuracy is maintained.

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

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

individual, the matter should be referred to the Headteacher 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 school will keep student data until the student reaches the age of 25. Student data, other than name and registration information, will be deleted or disposed of after this point unless required to be held longer by legislation. Student name and registration data may be kept indefinitely. Staff personal data will be retained for 7 years after the person has left the employ of the school. Staff names and basic employment history (start and end dates and positions held) may be held indefinitely. Unless part of a student or staff record, files and other papers (either in hard copy or electronic format) relating to specific events which contain sensitive data (e.g. passport details) should be securely destroyed or deleted within 12 months of the end of the event, unless there is a justifiable reason to retain it for longer. This must be at the judgement of the relevant member of staff who is personally accountable for such a decision and the specific circumstances are to be recorded in the Data Register. *Staff must not retain copies of personal data on personal drives or local files once their immediate use has finished; any need to retain such data for archive or record purposes are to be met by central storage; ie in student/staff records or departmental drives which are recorded in the Data Register.*

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. 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 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.
    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 Support Staff Director 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. 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 and other schools in accordance with legislation and these examples are described in the Privacy Notices at Annex B, C and D. Other instances, where there is a lawful basis of Legitimate Interest to transmit data to third parties, must be recorded in the Data Register and consideration given as to whether it would be also appropriate to obtain positive consent from the subject.

32. 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.
- Personal data on USB pens, 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 Suite 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.

33. 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 to the DPL*. See Annex F for the Data Breach Procedure.

34. Implementation: The Headteacher 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, DPL or the Headteacher.

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. The school provides a form for such requests that is designed to collect the information needed to identify the data you are requesting. Download and complete the form and then 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 DPO@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
- photographic identification
- details of the information required

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.

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:

- Head's PA – 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.

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, 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.

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
Privacy Notice (for students and their families)

Aylesbury High School is the *data controller* of the personal information you provide to us. This means the school determines the purposes for which, and the manner in which, any personal data relating to students and their families is to be processed. The Data Protection Lead, Mr K Marshall, acts as the representative for the school with regard to its data controller responsibilities and can be contacted on 01296 388222 or DPO@ahs.bucks.sch.uk.

Mr C King is the Data Protection Officer. His role is to oversee and monitor the school's data protection procedures, and to ensure they are compliant with the GDPR. The Data Protection Officer can be contacted at DPO@ahs.bucks.sch.uk.

If you need to tell the School about an update for your personal data then please contact the relevant Pastoral Support Assistant for you/your daughter's Key Stage or use office@ahs.bucks.sch.uk.

Why do we collect and use your information?
Aylesbury High School holds the legal right to collect and use personal data relating to students and their families and we may also receive information regarding them from their previous school, Local Authority and/or the DfE. We collect and use personal data in order to meet legal requirements and legitimate interests set out in the GDPR and UK law, including those in relation to the following:

- Article 6 and Article 9 of the GDPR
- Education Act 1996
- Regulation 5 of The Education (Information About Individual students) (England) Regulations 2013

In accordance with the above, the personal data of students and their families is collected and used for the following reasons:

- to support student learning
- to monitor and report on student progress
- to provide appropriate pastoral care
- to assess the quality of our services
- to comply with the law regarding data sharing
- to enable students to quickly and easily access catering and library services

What data do we hold and use?
The categories of student information that we collect and use include:

- Personal information (such as name, unique student number, date of birth and address)
- Characteristics (such as ethnicity, language, nationality, country of birth and free school meal eligibility)
- Attendance information (such as sessions attended, number of absences and absence reasons)
- Biometric information (includes photographs and digital finger scans)
- Assessment information
- Relevant medical information
- Special educational needs information
- Exclusions / behavioural information

The categories of parent and other student contact information that we collect and use include:

- Personal information (such as name, date of birth and address)
- Contact information (such as email addresses and telephone numbers)
- Student relationship (information relating to your links to the student, such as your relationship to them)

We collect and process sensitive data (known as Special Category Data) such as special educational needs or safeguarding information where there is a legal obligation so to do or there is a legitimate interest in supporting a student's education and welfare. In such cases we ensure either the subject has given explicit consent or it is necessary to protect the vital interests of the data subject or of another person.

How long is your data stored for?
Personal data relating to students and their families is stored in line with the School's GDPR Data Protection Policy. In accordance with the GDPR, the school does not store personal data indefinitely; data is only stored for as long as is necessary to complete the task for which it was originally collected. We normally hold student data after they have left the School until they reach the age of 25.

Will my information be shared?
The school is required by UK Law to share student data with the DfE via statutory data collections; some of this information is then stored in the The National Pupil Database (NPD) which is managed by the DfE. The DfE may share information about our students from the NDP with third parties who promote the education or wellbeing of children in England by:

- Conducting research or analysis
- Producing statistics
- Providing information, advice or guidance

The DfE has robust processes in place to ensure the confidentiality of any data shared from the NDP is maintained.

The School also routinely shares student information with:

- schools that the student's attend after leaving us
- our local authority
- parents and legal guardians

This shared information includes the names, addresses and contact information of students' families, but does not include biometric information.

Once a student reaches the age of 13 we also pass student information to our local authority or their provider of youth support services, as they have responsibilities in relation to the education or training of 13-19 year olds under section 507B of the Education Act 1996. This enables them to provide youth support services and careers advice. A parent or guardian can request that only their child's name, address and date of birth is passed to their local authority or provider of youth support services by informing us. This right is transferred to the student once they reach the age of 16. We may also share specific personal data of students who are aged 16 and over with post-16 education and training providers, in order to secure appropriate services for them. The information

provided includes addresses and dates of birth of all students and their parents, and any information necessary to support the services, e.g. school name, ethnicity or gender.
In some cases, your data will be outsourced to a third party processor who will provide a service to us. We do this either to enhance student attainment through analysis of their achievement data or to enhance their school experience by providing services such as cashless catering, on-line payments or educational trips, or improve efficiency through quicker identity confirmation for registration or library services. The companies that we currently routinely use for such services include:

- Transfer testing applicant photos, family contact and medical information - The Bucks Grammar Schools
- Email and document storage - Google
- On-line payment and parent communications - ParentMail
- Parent communications - SchoolComms
- Library records - Oliver
- Cashless catering – Harrisons Catering Services Ltd and Nationwide Retail Services
- Accounts - SAGE
- Achievement analysis - Fischer Family Trust
- On-line assessment (eg CATS) - CEM

We have a legitimate reason for sharing this data with these companies and will only do so where we are satisfied that data will be protected and not misused. If you do not want us to pass personal data to such companies and we are able to comply with your request without prejudicing the school's operation or a student's education, we will comply with your request; we will explain to you the reasons if we cannot comply with this type of request.

What are your rights?
Parents and students have the following rights in relation to the processing of their personal data.

You have the right to:

- be informed about how we use your personal data
- request access to the personal data that we hold. To make a request for your personal information, or be given access to your child's educational record, contact the Data Manager at School
- request that your personal data is amended if it is inaccurate or incomplete
- request that your personal data is erased where there is no compelling reason for its continued processing
- request that the processing of your data is restricted in certain circumstances
- object to the processing of personal data that is likely to cause, or is causing, damage or distress
- prevent processing for the purpose of direct marketing

Where the processing of your data is based on your consent, you may withdraw this consent at any time.

Where can you find out more information?
If you would like to find out more information about how we use and store your personal data, please visit our website and download our GDPR Data Protection Policy.

If you have a concern about the way we are collecting or using your personal data, you should in the first instance let us know so that we can try and resolve your concern. If you

are unhappy with the way we respond you may use our Complaints Procedure and if still dissatisfied, you can raise a concern with the Information Commissioner's Office (ICO) - to find out how to contact them, please visit their website www.ico.org.uk.

Annex C
Privacy Notice (for the School's workforce)

Aylesbury High School is the *data controller* of the personal information you provide to us. This means the school determines the purposes for which, and the manner in which, any personal data relating to the school workforce and their families is to be processed. The Data Protection Lead, Mr K Marshall, acts as the representative for the school with regard to its data controller responsibilities and can be contacted on 01296 388222 or DPO@ahs.bucks.sch.uk.

Mr C King is the Data Protection Officer. His role is to oversee and monitor the school's data protection procedures, and to ensure they are compliant with the GDPR. The Data Protection Officer can be contacted at DPO@ahs.bucks.sch.uk.

If you need to tell the School about an update for your personal data, then please contact the Headteacher's PA.

Why do we collect and use your information?
Aylesbury High School holds the legal or legitimate right to collect and use personal data relating to employees, volunteers and other persons who work in the school.

We use school workforce data to:

- enable the development of a comprehensive picture of the workforce and how it is deployed
- inform the development of recruitment and retention policies
- enable individuals to be paid
- support individuals with disability or medical conditions at work
- manage absence and ill health issues
- enable staff to be recognised by other staff and students
- make staff access to areas of the school, catering and library services more easy and efficient

Whilst the majority of information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with data protection legislation, we will inform you whether you are required to provide certain school workforce information to us or if you have a choice in this.

What data do we hold and use?
The categories of school workforce information that we collect, process, hold and share include:

- personal information (such as name, employee or teacher number, national insurance number)
- special categories of data including characteristics information such as gender, age, ethnic group, disability and medical data
- contract information (such as start dates, hours worked, post, roles and salary information)
- work absence information (such as number of absences and reasons)
- qualifications (and, where relevant, subjects taught)
- Biometric information (photographs and digital finger scans)
- Information on criminal convictions provided through the Disclosure and Barring Service

We collect and process sensitive data (known as Special Category Data) such as medical needs or criminal conviction information where there is a legal obligation so to do or there is a legitimate interest in supporting a person's welfare. In such cases we ensure either the subject has given explicit consent or it is necessary to protect the vital interests of the data subject or of another person.

How long is your data stored for?
In accordance with the GDPR, the school does not store personal data indefinitely; data is only stored for as long as is necessary to complete the task for which it was originally collected. Personal data relating to the School's workforce is usually retained for 7 years to comply with HMRC audit requirements, after which time the personal data will be erased or destroyed. The basic contract information, ie who was employed in what role and when, will be retained indefinitely. Data relating to unsuccessful applicants will be retained for 6 months.

Will my information be shared?
We do not share information about workforce members with anyone without consent unless the law and our policies allow us to do so.

Department for Education (DfE)
We share personal data with the Department for Education (DfE) on a statutory basis. This data sharing underpins workforce policy monitoring, evaluation, links to school funding / expenditure and the assessment of educational attainment. We are required to share information about our staff with the (DfE) under section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments.

Payroll Bureau
We share basic data including name, address, National Insurance number and date of birth with our payroll provider as it is a legitimate requirement in order for them to process our payroll, inform the HMRC and pension bodies, and arrange payment for staff.

HMRC
We share basic data including name, address, National Insurance number and date of birth with the HMRC because we have legal obligation to notify them of payments made and to enable them to collect the correct National Insurance and tax payments from staff.

Pension Bodies
We share basic data including name, address, National Insurance number and date of birth with pension bodies, as it is a legitimate requirement in order to allow them to manage staff pensions.

Third Party Service Providers
We share basic personal data (such as name, address and date of birth) with third party service providers, as it is needed to enable their systems to identify the staff user and communicate with them or provide the service to staff for which we have contacted with them. We routinely share data as follows:

- email and document storage systems - Google
- on-line payment and automated communications - ParentMail
- library records - Oliver
- cashless catering – Harrisons Catering Services Ltd and Nationwide Retail Services
- accounts - SAGE

We have a legitimate reason for sharing this data with these commercial companies and

will only do so where we are satisfied that data will be protected and not misused. If you do not want us to pass personal data to such companies and we are able to comply with your request without prejudicing the school's operation, we will comply with your request; we will explain to you the reasons if we cannot comply with this type of request.

What are your rights?
Staff, volunteers and other school workers have the following rights in relation to the processing of their personal data.

You have the right to:

- be informed about how we use your personal data.
- request access to the personal data that we hold. To make a request for your personal information, or be given access to your child's educational record, contact the Data Manager at School.
- request that your personal data is amended if it is inaccurate or incomplete.
- request that your personal data is erased where there is no compelling reason for its continued processing.
- request that the processing of your data is restricted in certain circumstances.
- object to the processing of personal data that is likely to cause, or is causing, damage or distress
- prevent processing for the purpose of direct marketing

Where the processing of your data is based on your consent, you may withdraw this consent at any time.

Where can you find out more information?
If you would like to find out more information about how we use and store your personal data, please visit our website and download our GDPR Data Protection Policy.

If you have a concern about the way we are collecting or using your personal data, you should in the first instance let us know so that we can try and resolve your concern. If you are unhappy with the way we respond you may use our Complaints Procedure and if still dissatisfied, you can raise a concern with the Information Commissioner's Office (ICO) - to find out how to contact them, please visit their website www.ico.org.uk.

Annex D
Privacy Notice (for the School's Donors and Alumni)

Aylesbury High School is the *data controller* of the personal information you provide to us. This means the school determines the purposes for which, and the manner in which, any personal data relating to donors to the school and Alumni is to be processed. The Data Protection Lead, Mr K Marshall, acts as the representative for the school with regard to its data controller responsibilities and can be contacted on 01296 388222 or DPO@ahs.bucks.sch.uk.

Mr C King is the Data Protection Officer. His role is to oversee and monitor the school's data protection procedures, and to ensure they are compliant with the GDPR. The Data Protection Officer can be contacted at DPO@ahs.bucks.sch.uk.

If you need to tell the School about an update for your personal data then please contact the Development and Alumni Relations Department at the School.

Development and Alumni Relations Privacy Statement

The aim of this Privacy Notice
Our alumni and supporters are extremely important to us and this Privacy Notice explains how Aylesbury High School's Development and Alumni Relations Department collects, stores, manages and protects your data. It outlines the types of data that we hold and how we use it to provide services to our alumni and supporters. We aim to be clear when we collect your personal information and not do anything you would not reasonably expect.

Who we are and what we do
The Development and Alumni Relations Department supports Aylesbury High School through contact with alumni, students, and supporters of the school. We do this by offering a range of academic, social and networking events and publications. We also fundraise to support the school's students, teaching, research and capital projects.

In order to do this, we have a database that contains personal data collected by the school during the course of our relationship with students, alumni, donors and supporters. Initially, data about students is transferred into our database from the student record system. The vast majority of the information we hold is obtained directly from you and we always aim to keep your details up to date, and to check that the contact details we have for you are correct, and, where appropriate, update them. As a result, some of the data may also have been obtained from publicly available sources – for example, we may find a new address for you by using the Royal Mail's National Change of Address database (NCOA). We value our relationship with you and we use your personal data to ensure we contact you in the most appropriate way and to ensure we work efficiently and effectively.

Our responsibilities and legal basis for processing your data
As part of our work we process and store personal information relating to students, staff, alumni, current and potential supporters and friends of Aylesbury High School and we therefore adhere to the Data Protection Act 2018 and General Data Protection Regulation (GDPR. We take our responsibilities under this Act seriously and ensure the personal information we obtain is held, used, transferred and processed in accordance with the Act.

Aylesbury High School's Development and Alumni Relations Department processes the information outlined in this Privacy Notice in pursuit of our legitimate interests in:

- Communicating with students, staff, alumni, and current and potential supporters
- Providing benefits and services to students, staff, alumni and supporters
- Furthering the school's educational charitable mission (which includes fundraising and securing the support of volunteers)
- Enabling the school to achieve its strategic and operational goals

We may pursue these legitimate interests by contacting you by email, post or social media. Information about how you can manage the ways that we contact you, including how to opt out from some or all contact from the Development and Alumni Relations Department, is outlined in the 'Your rights' section below.

Whilst Aylesbury High School relies on legitimate interest as the legal basis for processing, where this is not overridden by the interests and rights or freedoms of the data subjects concerned, it recognises that it is not the only lawful ground for processing data. As such, where appropriate, Aylesbury High School's Development and Alumni Relations Department will sometimes process your data on an alternative legal basis – for example, because you have given us consent to do so.

The data we hold

The personal data the Development and Alumni Relations Department stores and processes, which is given to us by our alumni, may include:

- Name, title and gender
- Contact details including postal address, email address, phone number and links to social media accounts (LinkedIn)
- Information about your time at the school and other academic institutions
- Your occupation and professional activities
- Your interests supporting the school
- Your relationships to other alumni, supporters and friends
- Records of donations and Gift Aid status, where applicable (as required by HMRC)
- Records of communications sent to you by the Development and Alumni Relations Department or received from you
- Volunteering by you on behalf of the school
- Media articles about you
- Archived photographs
- information on your engagement in school meetings, events, groups or networks

How we use your data

Unless you have requested otherwise, your data may be used and processed for a full range of alumni engagement and fundraising purposes. These include the following communications and marketing activities, which may be sent by mail, email, telephone and social media:

- School publications
- Notification of alumni events
- Fundraising programmes
- Promotion of alumni and student mentoring initiatives.

The school may use third-party partners to support the activities described above. The receipt of data by the Development and Alumni Relations Department in this manner is subject to the third party's own privacy policy. A list of parties with whom we partner in this way is available on request. Data obtained in this way is treated no differently to any

other once held by Development and Alumni Relations Department, and is bound by the terms of this Privacy Notice as soon as it is received.
We may carry out projects to find new contact details for alumni with whom we are not in contact, to ensure the school can remain in touch with as many of its alumni as possible. If you provide us with contact details for a particular method of communication we will assume that you have given us your consent for us to update your record and communicate with you using this information, unless you have told us otherwise. Contact details provided directly by you will update any previous preferences in relation to this channel unless you inform us otherwise. If you are registered with the Telephone Preference Service (TPS) but provide us with a telephone number, we will assume that we have your consent to call you on this number. Fundraising is a key part of the Development and Alumni Relations Department, and we are committed to working in a transparent, ethical, responsible and honest way.

Protecting your data
We are committed to holding your data securely and treating it with sensitivity. All data is held securely and in accordance with the Data Protection Act 2018 and General Data Protection Regulations (GDPR). Your data is held on a database hosted on a secure server within the school network. This database is protected by multi-level authentication and access is restricted to individuals who need to see the data to carry out their duties at the school. This is limited to: members of staff in the Development and Alumni Relations Department; assigned IT support; and colleagues from other areas within the school who work closely with the Development and Alumni Relations Department on the provision of services to alumni and supporters, such as the Careers Coordinators. User access rights to the database are restricted according to individual job roles in order to ensure that users only see information relevant to them. This access is reviewed on a regular basis.

Unless we have a legal obligation to do so, we will not disclose your data to individuals, organisations or other entities outside the school. All external entities with whom data is being shared and to whom we are not legally bound must sign a contract and/or a confidentiality and non-disclosure agreement before any data transfer takes place. We do not sell to or trade your data with any other organisations.

Your rights
The Development and Alumni Relations Department considers its relationship with alumni and supporters to be lifelong, and we will hold your details until you tell us you no longer wish to hear from us. We will always try to ensure that the data we hold for you is up to date, reasonable and not excessive. You will always have the right to:

- be informed as to how we use your data (via this Privacy Notice);
- access or request a copy of the data we hold about you;
- update, amend or rectify the data we hold about you
- change your communication preferences at any time to restrict how we process your data, or opt out of some or all communication from Development and Alumni Relations Department
- ask us to remove your data from our records
- withdraw consent, where it is used as a legal basis for processing
- object to or restrict the processing of your information for any of the purposes outlined above.

If you have any questions about this Privacy Notice, or would like to receive a copy of the information we hold about you, please contact us at: Development and Alumni Relations, Aylesbury High School, Walton Road, Aylesbury, HP21 7SX, or telephone 01296 388222

Future changes
From time to time, we may use your information for new purposes not currently described in this Privacy Notice. If our information practices change at some time in the future, we will always inform you of policy changes.

Annex E
Privacy Notice (for the School's Hirers and other short term visitors)

Aylesbury High School is the *data controller* of the personal information you provide to us. This means the school determines the purposes for which, and the manner in which, any personal data relating to the school workforce and their families is to be processed. The Data Protection Lead, Mr K Marshall, acts as the representative for the school with regard to its data controller responsibilities and can be contacted on 01296 388222 or DPO@ahs.bucks.sch.uk.

Mr C King is the Data Protection Officer. His role is to oversee and monitor the school's data protection procedures, and to ensure they are compliant with the GDPR. The Data Protection Officer can be contacted at DPO@ahs.bucks.sch.uk.

If you need to tell the School about an update for your personal data then please contact the Headteacher's PA.

Why do we collect and use your information?
Aylesbury High School holds the legal or legitimate right to collect and use personal data relating to people who make use of the School's premises or visit the school.

We use data to:

- manage the safety of all persons on the site
- manage availability of resources, such as parking
- enable us to communicate with our hirers and visitors

Information is provided to us on a voluntary basis but if it is not provided the School reserves the right to refuse access. Because of the nature of the information held, specific records of consent are not required.

What data do we hold and use?
The categories of school workforce information that we collect, process, hold and share include:

- basic personal information (such as name and contact information)
- information on vehicle registration

How long is your data stored for?
In accordance with the GDPR, the school does not store personal data indefinitely; data is only stored for as long as is necessary to complete the task for which it was originally collected. Personal data relating to the School's activity is usually retained for up to 7 years to comply with HMRC legislation and safeguarding requirements, after which time the personal data will be erased or destroyed.

Will my information be shared?
We will not not share your personal information with anyone without consent unless the law and our policies allow us to do so.

What are your rights?
People visiting the school site have the following rights in relation to the processing of their personal data.

You have the right to:

- be informed about how we use your personal data.
- request access to the personal data that we hold. To make a request for your personal information, contact the Facilities Administrator.
- request that your personal data is amended if it is inaccurate or incomplete.
- request that your personal data is erased where there is no compelling reason for its continued processing.
- request that the processing of your data is restricted in certain circumstances.
- object to the processing of personal data that is likely to cause, or is causing, damage or distress
- prevent processing for the purpose of direct marketing

Where the processing of your data is based on your consent, you may withdraw this consent at any time.

Where can you find out more information?
If you would like to find out more information about how we use and store your personal data, please visit our website and download our GDPR Data Protection Policy.

If you have a concern about the way we are collecting or using your personal data, you should in the first instance let us know so that we can try and resolve your concern. If you are unhappy with the way we respond you may use our Complaints Procedure and if still dissatisfied, you can raise a concern with the Information Commissioner's Office (ICO) - to find out how to contact them, please visit their website www.ico.org.uk.

Annex F
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 Headteacher/Deputy Headteacher. The DPL will at the first opportunity inform the Headteacher. 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 Headteacher 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 Headteacher 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 Headteacher, 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 Headteacher will need to decide if the breach warrants a disciplinary investigation.