Data Protection Policy

1. Policy statement

Uxbridge High School Academy Trust has a legal duty to ensure that the school processes personal information in a way which is compliant with data protection laws.

We take the protection and security of all personal data held by the school very seriously, and as such has adopted this policy to set out our rules on data protection and the legal conditions that must be satisfied in relation to the obtaining, handling, processing, storage, transportation and destruction of personal information held by the school.

Everyone has rights with regard to the way in which their personal data is handled. During the course of our activities as a school we will collect, store and process personal data about our students, workforce, parents, governors, visitors and others. This makes us a data controller in relation to that personal data.

We are committed to the protection of all personal data and special category personal data for which we are the data controller.

The law imposes significant fines for failing to lawfully process and safeguard personal data and failure to comply with this policy may result in those fines being applied.

All members of our workforce must comply with this policy when processing personal data on our behalf. Any breach of this policy may result in disciplinary or other action.

2. About this policy

The types of personal data that we may be required to handle include information about students, parents, our workforce, and others that we deal with. The personal data which we hold is subject to certain legal safeguards specified in the *General Data Protection Regulation* (GDPR) and other regulations (together 'Data Protection Legislation').

This policy also meets the requirements of the *Protection of Freedoms Act 2012* when referring to our use of biometric data, reflects the ICO's code of practice for the use of surveillance cameras and personal information, and complies with our funding agreement and articles of association.

This policy and any other documents referred to in it set out the basis on which we will process any personal data we collect from data subjects, or that is provided to us by data subjects or other sources. This policy applies to all personal data, regardless of whether it is in paper or electronic format.

This policy does not form part of any employee's contract of employment and may be amended at any time.

This policy sets out rules on data protection and the legal conditions that must be satisfied when we process personal data, and takes effect from 25th May 2018.

2.1 Definition of data protection terms

All defined terms in this policy are indicated in blue text, and a list of definitions is included in the Annex to this policy.

3. Roles and responsibilities

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

3.1 Governing body

The governing body has overall responsibility for ensuring that our school complies with all relevant data protection obligations.

3.2 Data protection officer

As an academy trust we are required to appoint a Data Protection Officer ("DPO"). Our DPO is Miss Norwena Thomas, who is contactable via email at dpo@uhs.org.uk.

The DPO is responsible for overseeing the implementation of this policy, monitoring compliance with the Data Protection Legislation and for developing related policies and guidelines where applicable. Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the DPO.

The DPO is also the central point of contact for all data subjects and others in relation to matters of data protection.

3.3 Principal

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

3.4 All staff

All staff at the school are responsible for:

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

4. Data protection principles

Anyone processing personal data must comply with the data protection principles. These provide that personal data must be:

- processed fairly and lawfully and transparently in relation to the data subject;
- processed for specified, lawful purposes and in a way which is not incompatible with those purposes;
- adequate, relevant and not excessive for the purpose;

- accurate and, where necessary, kept up to date;
- not kept for any longer than is necessary for the purpose; and
- processed securely using appropriate technical and organisational measures.

Personal data must also:
- be processed in line with data subjects' rights;
- not be transferred to people or organisations situated in other countries without adequate protection.

We will comply with these principles in relation to any processing of personal data by the school.

5. Fair and lawful processing

Data Protection Legislation is not intended to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the data subject.

For personal data to be processed fairly, data subjects must be made aware:
- that the personal data is being processed;
- why the personal data is being processed;
- what the lawful basis is for that processing (see below);
- whether the personal data will be shared, and if so with whom;
- the period for which the personal data will be held;
- the existence of the data subject's rights in relation to the processing of that personal data; and
- the right of the data subject to raise a complaint with the Information Commissioner's Office (the ICO) in relation to any processing.

We will only obtain such personal data as is necessary and relevant to the purpose for which it was gathered, and will ensure that we have a lawful basis for any processing.

For personal data to be processed lawfully, it must be processed on the basis of one of the legal grounds set out in the Data Protection Legislation. We will normally process personal data under the following legal grounds:
- where the processing is necessary for the performance of a contract between us and the data subject, such as an employment contract;
- where the processing is necessary to comply with a legal obligation that we are subject to, e.g. the Education Act 2011;
- where the law otherwise allows us to process the personal data or we are carrying out a task in the public interest; and
- where none of the above apply then we will seek the consent of the data subject to the processing of their personal data.

When special category personal data is being processed then an additional legal ground must apply to that processing. We will normally only process special category personal data under the following legal grounds:
- where the processing is necessary for employment law purposes, for example in relation to sickness absence;
- where the processing is necessary for reasons of substantial public interest, for example for the purposes of equality of opportunity and treatment;
- where the processing is necessary for health or social care purposes, for example in relation to students with medical conditions or disabilities; and

- where none of the above apply then we will seek the consent of the data subject to the processing of their special category personal data.

We will inform data subjects of the above matters by way of appropriate privacy notices which shall be provided to them when we collect the data or as soon as possible thereafter, unless we have already provided this information such as at the time when a student joins us.

If any data user is in doubt as to whether they can use any personal data for any purpose then they must contact the DPO before doing so.

5.1 Vital interests

There may be circumstances where it is considered necessary to process personal data or special category personal data in order to protect the vital interests of a data subject. This might include medical emergencies where the data subject is not in a position to give consent to the processing. We believe that this will only occur in very specific and limited circumstances. In such circumstances we would usually seek to consult with the DPO in advance, although there may be emergency situations where this does not occur.

5.2 Consent

Where none of the other bases for processing set out above apply then the school must seek the consent of the data subject before processing any personal data for any purpose.

There are strict legal requirements in relation to the form of consent that must be obtained from data subjects.

When students and/or our workforce join the school a consent form will be required to be completed in relation to them. This consent form deals with the taking and use of photographs and videos of them, amongst other things. Where appropriate third parties may also be required to complete a consent form.

In relation to all students under the age of 12 years old we will seek consent from an individual with parental responsibility for that student.

We will generally seek consent directly from a student who has reached the age of 12, however we recognise that this may not be appropriate in certain circumstances and therefore may be required to seek consent from an individual with parental responsibility.

If consent is required for any other processing of personal data of any data subject then the form of this consent must:

- inform the data subject of exactly what we intend to do with their personal data;
- require them to positively confirm that they consent – we cannot ask them to opt-out rather than opt-in; and
- inform the data subject of how they can withdraw their consent.

Any consent must be freely given, which means that we cannot make the provision of any goods or services or other matter conditional on a data subject giving their consent.

The DPO must always be consulted in relation to any consent form before consent is obtained.

A record must always be kept of any consent, including how it was obtained and when.

6. Processing for limited purposes

In the course of our activities as a school, we may collect and process the personal data set out in our Schedule of Processing Activities. This may include personal data we receive directly from a data subject (for example, by completing forms or by corresponding with us by mail, phone, email or otherwise) and personal data we receive from other sources (including, for example, local authorities, other schools, parents, other students or members of our workforce).

We will only process personal data for the specific purposes set out in our Schedule of Processing Activities or for any other purposes specifically permitted by Data Protection Legislation or for which specific consent has been provided by the data subject.

7. Notifying data subjects

If we collect personal data directly from data subjects, we will inform them about:

- our identity and contact details as data controller and those of the DPO;
- the purpose or purposes and legal basis for which we intend to process that personal data;
- the types of third parties, if any, with which we will share or to which we will disclose that personal data;
- whether the personal data will be transferred outside the European Economic Area (EEA) and if so the safeguards in place;
- the period for which their personal data will be stored, by reference to our Retention and Destruction Policy;
- the existence of any automated decision making in the processing of the personal data along with the significance and envisaged consequences of the processing and the right to object to such decision making; and
- the rights of the data subject to object to or limit processing, request information, request deletion of information or lodge a complaint with the ICO.

Unless we have already informed data subjects that we will be obtaining information about them from third parties (for example in our privacy notices), then if we receive personal data about a data subject from other sources, we will provide the data subject with the above information as soon as possible thereafter, informing them of where the personal data was obtained from.

8. Adequate, relevant and non-excessive processing

We will only collect personal data to the extent that it is required for the specific purpose notified to the data subject, unless otherwise permitted by Data Protection Legislation.

9. Accurate data

We will ensure that personal data we hold is accurate and kept up to date.

We will take reasonable steps to destroy or amend inaccurate or out-of-date data.

Data subjects have a right to have any inaccurate personal data rectified. See further below in relation to the exercise of this right.

10. Timely processing

We will not keep personal data longer than is necessary for the purpose or purposes for which they were collected. We will take all reasonable steps to destroy, or erase from our systems, all personal data which is no longer required.

11. Processing in line with data subject's rights

We will process all personal data in line with data subjects' rights, in particular their right to:

- request access to any personal data we hold about them;
- object to the processing of their personal data, including the right to object to direct marketing;
- have inaccurate or incomplete personal data about them rectified;
- restrict processing of their personal data;
- have personal data we hold about them erased
- have their personal data transferred; and
- object to the making of decisions about them by automated means.

11.1 The right of access to personal data

Data subjects may request access to all personal data we hold about them. Such requests will be considered in line with the schools *Subject Access Request Procedure*.

11.2 The right to object

In certain circumstances data subjects may object to us processing their personal data. This right may be exercised in relation to processing that we are undertaking on the basis of a legitimate interest or in pursuit of a statutory function or task carried out in the public interest.

An objection to processing must be in writing with clear reasons as to why the data subject objects, and should be address to the DPO. Such an objection does not have to be complied with where the school can demonstrate compelling legitimate grounds which override the rights of the data subject.

Such considerations are complex and must always be referred to the DPO upon receipt of the request to exercise this right.

In respect of direct marketing any objection to processing must be complied with.

The school is not however obliged to comply with a request where the personal data is required in relation to any claim or legal proceedings.

11.3 The right to rectification

If a data subject informs the school that personal data held about them by the school is inaccurate or incomplete then we will consider that request and provide a response within one month.

If we consider the issue to be too complex to resolve within that period then we may extend the response period by a further two months. If this is necessary then we will inform the data subject within one month of their request that this is the case.

We may determine that any changes proposed by the data subject should not be made. If this is the case then we will explain to the data subject why this is the case. In those circumstances we will inform the data subject of their right to complain to the ICO at the time that we inform them of our decision in relation to their request.

11.4 The right to restrict processing

Data subjects have a right to "block" or suppress the processing of personal data. This means that the school can continue to hold the personal data but not do anything else with it.

The school must restrict the processing of personal data:

- where it is in the process of considering a request for personal data to be rectified (see above);
- where the school is in the process of considering an objection to processing by a data subject;
- where the processing is unlawful but the data subject has asked the school not to delete the personal data; and
- where the school no longer needs the personal data but the data subject has asked the school not to delete the personal data because they need it in relation to a legal claim, including any potential claim against the school.

If the school has shared the relevant personal data with any other organisation then we will contact those organisations to inform them of any restriction, unless this proves impossible or involves a disproportionate effort.

The DPO must be consulted in relation to requests under this right.

11.5 The right to be forgotten

Data subjects have a right to have personal data about them held by the school erased only in the following circumstances:

- where the personal data is no longer necessary for the purpose for which it was originally collected;
- when a data subject withdraws consent – which will apply only where the school is relying on the individual's consent to the processing in the first place;
- when a data subject objects to the processing and there is no overriding legitimate interest to continue that processing – see above in relation to the right to object;
- where the processing of the personal data is otherwise unlawful;
- when it is necessary to erase the personal data to comply with a legal obligation.

The school is not required to comply with a request by a data subject to erase their personal data if the processing is taking place:

- to exercise the right of freedom of expression or information;
- to comply with a legal obligation for the performance of a task in the public interest or in accordance with the law;
- for public health purposes in the public interest;
- for archiving purposes in the public interest, research or statistical purposes; or
- in relation to a legal claim.

If the school has shared the relevant personal data with any other organisation then we will contact those organisations to inform them of any erasure, unless this proves impossible or involves a disproportionate effort.

The DPO must be consulted in relation to requests under this right.

11.6 Right to data portability

In limited circumstances a data subject has a right to receive their personal data in a machine readable format, and to have this transferred to other organisations.

If such a request is made then the DPO must be consulted.

12. Data security

We will take appropriate security measures against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.

We will put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. Security procedures are detailed in the school's *Managing ICT and E-Safety Policy.*

Any member of staff found to be in breach of the security measures detailed in the *Managing ICT and E-Safety Policy* may be subject to disciplinary action.

13. Data protection impact assessments

The school takes data protection very seriously, and will consider and comply with the requirements of Data Protection Legislation in relation to all of its activities whenever these involve the use of personal data, in accordance with the principles of data protection by design and default.

In certain circumstances the law requires us to carry out detailed assessments of proposed processing. This includes where we intend to use new technologies which might pose a high risk to the rights of data subjects because of the types of data we will be processing or the way that we intend to do so.

The school will complete an assessment of any such proposed processing and has a template document which ensures that all relevant matters are considered.

The DPO should always be consulted as to whether a data protection impact assessment is required, and if so how to undertake that assessment.

14. Disclosure and sharing of personal information

We may share personal data that we hold about data subjects, and without their consent, with other organisations. Such organisations include the Department for Education, and/or the Education and Skills Funding Agency "ESFA", Ofsted, health authorities and health care professionals, the Local Authority, examination bodies, other schools, and other organisations where we have a lawful basis for doing so.

The school will inform data subjects of any sharing of their personal data unless we are not legally required to do so, for example where personal data is shared with the police in the investigation of a criminal offence.

In some circumstances we will not share safeguarding information. Please refer to our *Child Protection/ Safeguarding Children Policy*.

Further detail is provided in our Schedule of Processing Activities.

15. Data processors

We contract with various organisations who provide services to the school, including:

- payroll providers;
- cashless catering systems;
- biometric registration systems;
- behaviour monitoring systems;
- attendance monitoring systems;
- online homework and teaching resources/systems;
- rewards systems.

In order that these services can be provided effectively we are required to transfer personal data of data subjects to these data processors.

Personal data will only be transferred to a data processor if they agree to comply with our procedures and policies in relation to data security, or if they put in place adequate measures themselves to the satisfaction of the school. The school will always undertake due diligence of any data processor before transferring the personal data of data subjects to them.

Contracts with data processors will comply with Data Protection Legislation and contain explicit obligations on the data processor to ensure compliance with the Data Protection Legislation, and compliance with the rights of data subjects.

16. Images and videos

As part of our school activities, we may take photographs and record images of individuals within our school. As a school we want to celebrate the achievements of our students and therefore may want to use images and videos of our students within promotional materials, or for publication in the media such as local, or even national, newspapers covering school events or achievements. We will seek the consent of students, and their parents where appropriate, before allowing the use of images or videos of students for such purposes.

Whenever a student begins their attendance at the school they, or their parent(s)/carer(s) where appropriate, will be asked to complete a consent form in relation to the use of images and videos of that student. We will not use images or videos of students for any purpose where we do not have consent.

Parents and others attending school events are allowed to take photographs and videos of those events for domestic purposes. For example, parents can take video recordings of a school performance involving their child. The school does not prohibit this as a matter of policy. The school does not however agree to any such photographs or videos being used for any other purpose, but acknowledges that such matters are, for the most part, outside of the ability of the school to prevent.

The school asks that parents and others do not post any images or videos which include any child other than their own child on any social media or otherwise publish those images or videos.

17. Biometric recognition

At Uxbridge High School we use a cashless catering system which means that meals are paid for using biometrics (i.e. fingerprint recognition). The system works by turning an image of a student or staff member's fingerprint into a personalised reference. The reference only contains numbers and letters and does not keep the image of the fingerprint. The personalised

fingerprint reference of the student is stored securely on the school's system. Biometrics are used to pay for meals, stationery and to access the school's printing system.

Where biometric data is used as part of an automated biometric recognition system we will comply with the requirements of the *Protection of Freedoms Act 2012*.

The school will seek written consent from at least one parent or carer before we take any biometric data from a student to process. Parents/Carers and students have the right to choose not to use the school's biometric system(s). We will provide alternative means of accessing the relevant services for those students. For example students can pay for school dinners using their school ID card if they wish.

Parents/Carers and students can object to participation in the school's biometric recognition system(s) or withdraw consent, at any time, and we will make sure that any relevant data already captured is deleted.

As required by law, if a student refuses to participate in, or continue to participate in, the processing of their biometric data, we will not process that data irrespective of any consent given by the student's parent(s)/carer(s).

Where staff members and other adults use the school's biometric system(s), we will also obtain their consent before they first take part in it, and provide alternative means of accessing the relevant service if they object. Staff and other adults can also withdraw consent at any time, and the school will delete any relevant data already captured.

18. CCTV

The school operates a CCTV system. CCTV is located in various locations around the school site to ensure it remains safe. We will adhere to the ICO's code of practice for the use of CCTV.

We do not need to ask individual's permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

Please refer to the school's *CCTV Policy* for further details.

19. Changes to this policy

We may change this policy at any time. Where appropriate, we will notify data subjects of those changes.

ANNEX 1

Definitions

Term	Definition
Data	is information which is stored electronically, on a computer, or in certain paper-based filing systems.
Data controllers	are the people who or organisations which determine the purposes for which, and the manner in which, any personal data is processed. They are responsible for establishing practices and policies in line with Data Protection Legislation. We are the data controller of all personal data used in our business for our own commercial purposes.
Data processors	include any person or organisation that is not a data user that processes personal data on our behalf and on our instructions.
Data subjects	for the purpose of this policy include all living individuals about whom we hold personal data. This includes students, our workforce, staff, and other individuals. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal information.
Data users	are those of our workforce (including governors and volunteers) whose work involves processing personal data. Data users must protect the data they handle in accordance with this data protection policy and any applicable data security procedures at all times.
Personal data	means any information relating to an identified or identifiable natural person (a data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
Special category personal data	includes information about a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, physical or mental health or sexual life, or genetic or biometric data.
Personal data breach	is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.
Processing	is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. Processing also includes transferring personal data to third parties.
Workforce	includes, any individual employed by the school such as staff and those who volunteer in any capacity including governors.

APPENDIX 1

Subject access requests policy

1. Policy statement

All data subjects have rights of access to their personal data. This document sets out the procedure to be followed in relation to any requests made for the disclosure of personal data processed by the school.

2. Recognising a subject access request

As the school processes personal data concerning data subjects, those data subjects have the right to access that personal data under Data Protection Law. A request to access this personal data is known as a subject access request or SAR.

A data subject is generally only entitled to access their own personal data, and not to information relating to other people.

Any request by a data subject for access to their personal data is a SAR. This includes requests received in writing, by email, and verbally.

If any member of our workforce receives a request for information they should inform the Data Protection Officer (DPO) as soon as possible.

In order that the school is properly able to understand the nature of any SAR and to verify the identity of the requester, any requester making a request verbally should be asked to put their request in writing and direct this to the DPO.

A SAR will be considered and responded to in accordance with the Data Protection Law.

Any SAR must be notified to the DPO at the earliest opportunity.

3. Verifying the identity of a requester

The school is entitled to request additional information from a requester in order to verify whether the requester is in fact who they say they are.

Where the school has reasonable doubts as to the identity of the individual making the request, evidence of identity may be established by production of two or more of the following:

- current passport;
- current driving licence;
- recent utility bills with current address;
- birth/marriage certificate;
- P45/P60;
- recent credit card or mortgage statement.

If the school is not satisfied as to the identity of the requester then the request will not be complied with, so as to avoid the potential for an inadvertent disclosure of personal data resulting in a data breach.

4. Fee for responding to requests

The school will usually deal with a SAR free of charge.

Where a request is considered to be manifestly unfounded or excessive a fee may be requested. Alternatively, the school may refuse to respond to the request. If a request is considered to be manifestly unfounded or unreasonable the school will inform the requester why this is considered to be the case.

A fee may also be requested in relation to repeat requests for copies of the same information. In these circumstances a reasonable fee will be charged taking into account the administrative costs of providing the information.

5. Time period for responding to a SAR

The school has one month to respond to a SAR. This will run from the later of a) the date of the request, b) the date when any additional identification (or other) information requested is received, or c) payment of any required fee.

In circumstances where the school is in any reasonable doubt as to the identity of the requester, this period will not commence unless and until sufficient information has been provided by the requester as to their identity, and in the case of a third party requester the written authorisation of the data subject has been received (see below in relation to sharing information with third parties).

The period for response may be extended by a further two calendar months in relation to complex requests. What constitutes a complex request will depend on the particular nature of the request. The DPO must always be consulted in determining whether a request is sufficiently complex as to extend the response period.

Where a request is considered to be sufficiently complex as to require an extension of the period for response, the school will notify the requester within one calendar month of receiving the request, together with reasons as to why this is considered necessary.

A request may be received during or less than one month prior to a school holiday. Where a request is made prior to a holiday period the school will seek to respond prior to that holiday commencing, however where this is not possible then the school will inform the requester that this is the case.

Form of response

A requester can request a response in a particular form. In particular where a request is made by electronic means then, unless the requester has stated otherwise, the information should be provided in a commonly readable format.

6. Sharing information with third parties

Data subjects can ask that you share their personal data with another person such as an appointed representative (in such cases you should request written authorisation signed by the data subject confirming which of their personal data they would like you to share with the other person).

Equally if a request is made by a person seeking the personal data of a data subject, and which purports to be made on behalf of that data subject, then a response must not be provided unless and until written authorisation has been provided by the data subject. The school should not approach the data subject directly but should inform the requester that it cannot respond without the written authorisation of the data subject.

If the school is in any doubt or has any concerns as to providing the personal data of the data subject to the third party, then it should provide the information requested directly to the data subject. It is then a matter for the data subject to decide whether to share this information with any third party.

Personal data belongs to the data subject, and in the case of the personal data of a child regardless of their age the rights in relation to that personal data are theirs and not those of their parents. Parents, in most cases, do not have automatic rights to the personal data of their child.

However, there are circumstances where a parent can request the personal data of their child without requiring the consent of the child. This will depend on the maturity of the child and whether the school is confident that the child can understand their rights. Generally, where a child is under 12 years of age they are deemed not to be sufficiently mature as to understand their rights of access and a parent can request access to their personal data on their behalf.

In relation to a child 12 years of age or older, then provided that the school is confident that they understand their rights, and there is no reason to believe that the child does not have the capacity to make a request on their own behalf, the school will require the written authorisation of the child before responding to the requester, or provide the personal data directly to the child in accordance with the process above.

In all cases the school should consider the particular circumstances of the case, and the above are guidelines only.

7. Withholding information

There are circumstances where information can be withheld pursuant to a SAR. These are specific exemptions and requests should be considered on a case by case basis.

Where the information sought contains the personal data of third party data subjects then the school will:

- consider whether it is possible to redact information so that this does not identify those third parties, taking into account that it may be possible to identify third parties from remaining information;
- if this is not possible, consider whether the consent of those third parties can be obtained; and
- if consent has been refused, or it is not considered appropriate to seek that consent, then to consider whether it would be reasonable in the circumstances to disclose the information relating to those third parties. If it is not then the information may be withheld.

So far as possible the school will inform the requester of the reasons why any information has been withheld.

Where providing a copy of the information requested would involve disproportionate effort the school will inform the requester, advising whether it would be possible for them to view the documents at the school or seeking further detail from the requester as to what they are seeking, for example key word searches that could be conducted, to identify the information that is sought.

In certain circumstances information can be withheld from the requester, including a data subject, on the basis that it would cause serious harm to the data subject or another individual. If there are any concerns in this regard, then the DPO should be consulted.

8. Process for dealing with a subject access request (SAR)

When a SAR is received, the school will:

- notify the DPO who will be responsible for managing the response, and relevant department heads;
- acknowledge receipt of the request and provide an indication of the likely timescale for a response within 5 working days (use template);
- take all reasonable and proportionate steps to identify and disclose the data relating to the request;
- never delete information relating to a SAR, unless it would have been deleted in the ordinary course of events – it is an offence to amend or delete data following receipt of a SAR that would not have otherwise been so amended or deleted;
- consider whether to seek consent from any third parties which might be identifiable from the data being disclosed;
- seek legal advice, where necessary, to determine whether the school is required to comply with the request or supply the information sought;
- provide a written response, including an explanation of the types of data provided and, and as far as possible, for what reasons any data has been withheld (use template); and
- ensure that information disclosed is clear and technical terms are clarified and explained.

APPENDIX 2

Data Breach Notification Policy

1. Policy statement

Uxbridge High School is committed to the protection of all personal data and special category personal data for which we are the data controller.

The law imposes significant fines for failing to lawfully process and safeguard personal data and failure to comply with this policy may result in those fines being applied.

All members of our workforce must comply with this policy when processing personal data on our behalf. Any breach of this policy may result in disciplinary or other action.

2. About this policy

This policy informs all of our workforce on dealing with a suspected or identified data security breach.

In the event of a suspected or identified breach, the school must take steps to minimise the impact of the breach and prevent the breach from continuing or reoccurring.

Efficient internal management of any breach is required, to ensure swift and appropriate action is taken and confidentiality is maintained as far as possible.

The school must also comply with its legal and contractual requirements to notify other organisations including the Information Commissioner's Office (the ICO) and where appropriate data subjects whose personal data has been affected by the breach. This includes any communications with the press.

Failing to appropriately deal with and report data breaches can have serious consequences for the school and for data subjects including:

- identity fraud, financial loss, distress or physical harm;
- reputational damage to school; and
- fines imposed by the ICO.

3. Identifying a data breach

A data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

This could be the result of a breach of cyber security, such as a hack or virus, or it could be the result of a breach of physical security such as loss or theft of a mobile device or paper records. A data breach includes loss of data and so does not have to be the result of a conscious effort of a third party to access the data. Some examples of potential data breaches are listed below:

- Leaving a mobile device on a train;
- Theft of a bag containing paper documents;
- Destruction of the only copy of a document;
- Sending an email or attachment to the wrong recipient;
- Using an unauthorised email address to access personal data;
- Leaving paper documents containing personal data in a place accessible to other people.

4. Internal communication

Reporting a data breach upon discovery
If any member of our workforce suspects, or becomes aware, that a data breach may have occurred (either by them, another member of our workforce, a data processor, or any other individual) then they must contact the Data Protection Officer (the DPO) and their Leadership Line Manager immediately.

The data breach may need to be reported to the ICO, and notified to data subjects. This will depend on the risk to data subjects. The DPO must always be consulted in making a decision as to whether to report a data breach to the ICO. Initial investigations will inform as to whether the data breach should be reported.

If it is considered to be necessary to report a data breach to the ICO then the school must do so within 72 hours of discovery of the breach.

The school may also be contractually required to notify other organisations of the breach within a period following discovery.

It is therefore critically important that whenever a member of our workforce suspects that a data breach has occurred, this is reported internally to the DPO immediately.

Members of our workforce who fail to report a suspected data breach could face disciplinary or other action.

Investigating a suspected data breach
In relation to any suspected data breach the following steps must be taken as soon as possible. These do not have to be carried out as individual tasks, and the most appropriate way of dealing with any breach will depend on the nature of the breach and the information available at any time.

Breach minimisation
The first step must always be to identify how the data breach occurred, the extent of the data breach, and how this can be minimised. The focus will be on containing any data breach, and recovering any personal data. Relevant departments must be involved, such as IT, to take technical and practical steps where appropriate to minimise the breach. Appropriate measures may include:

- remote deactivation of school tablet devices;
- shutting down IT systems;
- contacting individuals to whom the information has been disclosed and asking them to delete the information; and
- recovering lost data.

Breach investigation:
When the school has taken appropriate steps to minimise the extent of the data breach it must commence an investigation as soon as possible to understand how and why the data breach occurred. This is critical to ensuring that a similar data breach does not occur again and to enable steps to be taken to prevent this from occurring.

Technical steps are likely to include investigating, using IT forensics where appropriate, to examine processes, networks and systems to discover:

- what data/systems were accessed;
- how the access occurred;
- how to fix vulnerabilities in the compromised processes or systems;
- how to address failings in controls or processes.

Other steps are likely to include discussing the matter with individuals involved to appreciate exactly what occurred and why, and reviewing policies and procedures.

Breach analysis
In order to determine the seriousness of a data breach and its potential impact on data subjects, and so as to inform the school as to whether the data breach should be reported to the ICO and notified to data subjects, it is necessary to analyse the nature of the data breach.

Such an analysis must include:
- the type and volume of personal data which was involved in the data breach;
- whether any special category personal data was involved;
- the likelihood of the personal data being accessed by unauthorised third parties;
- the security in place in relation to the personal data, including whether it was encrypted;
- the risks of damage or distress to the data subject.

The breach notification form annexed to this policy must be completed in every case of a suspected breach, and retained securely, whether or not a decision is ultimately made to report the data breach. This will act as evidence as to the considerations of the school in deciding whether or not to report the breach.

5. External communication
All external communication is to be managed and overseen by the DPO and the Principal.

Law Enforcement
The DPO and the Principal will assess whether the data breach incident requires reporting to any law enforcement agency, including the police. This will be informed by the investigation and analysis of the data breach, as set out above.

The DPO and the Principal shall coordinate communications with any law enforcement agency.

Other organisations
If the data breach involves personal data which we process on behalf of other organisations then we may be contractually required to notify them of the data breach.

The school will identify as part of its investigation of the data breach whether or not this is the case and any steps that must be taken as a result.

Information Commissioner's Office (The ICO)
If the school is the data controller in relation to the personal data involved in the data breach, which will be the position in most cases, then the school has 72 hours to notify the ICO if the data breach is determined to be notifiable.

A data breach is notifiable unless it is unlikely to result in a risk to the rights and freedoms of any individual. The DPO will make an assessment of the data breach against the following criteria taking into account the facts and circumstances in each instance:
- the type and volume of personal data which was involved in the data breach;

- whether any special category personal data was involved;
- the likelihood of the personal data being accessed by unauthorised third parties;
- the security in place in relation to the personal data, including whether it was encrypted;
- the risks of damage or distress to the data subject.

If a notification to the ICO is required then see section below on *Producing an ICO Breach Notification Report*.

Other supervisory authorities
If the data breach occurred in another country or involves data relating to data subjects from different countries then the DPO will assess whether notification is required to be made to supervisory authorities in those countries.

Data subjects
When the data breach is likely to result in a high risk to the rights and freedoms of the data subjects then the data subject must be notified without undue delay. This will be informed by the investigation of the breach by the school.

The communication will be coordinated by the DPO and will include at least the following information:
- a description in clear and plain language of the nature of the data breach;
- the name and contact details of the DPO;
- the likely consequences of the data breach;
- the measures taken or proposed to be taken by the school to address the data breach including, where appropriate, measures to mitigate its possible adverse effects.

There is no legal requirement to notify any individual if any of the following conditions are met:
- appropriate technical and organisational protection measures had been implemented and were applied to the data affected by the data breach, in particular, measures which render the data unintelligible to unauthorised persons (e.g. encryption);
- measures have been taken following the breach which ensure that the high risk to the rights and freedoms of the data subject is no longer likely to materialise;
- it would involve disproportionate effort to contact individuals. In which case a public communication or similar equally effective measure of communication to the data subjects shall be issued.

For any data breach, the ICO may mandate that communication is issued to data subjects, in which case such communication must be issued.

Press
Staff shall not communicate directly with the press and shall treat all potential data breaches as confidential unless otherwise instructed in writing by the DPO.

All press enquiries shall be directed to the Principal.

6. Producing an ICO Breach Notification Report
All members of our workforce are responsible for sharing all information relating to a data breach with the DPO, which will enable the Breach Notification Report Form to be completed.

When completing the Breach Notification Report Form all mandatory (*) fields must be completed, and as much detail as possible should be provided.

The DPO may require individuals involved in relation to a data breach to each complete relevant parts of the Breach Notification Form as part of the investigation into the data breach.

If any member of our workforce is unable to provide information when requested by the DPO then this should be clearly reflected in the Breach Notification Form together with an indication as to if and when such information may be available.

In the wake of a data protection breach, swift containment and recovery of the situation is vital. Every effort should be taken to minimise the potential impact on affected individuals, and details of the steps taken to achieve this should be included in this form.

The ICO requires that the school send the completed Breach Notification Form to casework@ico.org.uk, with 'DPA breach notification form' in the subject field, or by post to: The Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF.

7. Evaluation and response

Reporting is not the final step in relation to a data breach. The school will seek to learn from any data breach.

Therefore, following any breach an analysis will be conducted as to any steps that are required to prevent a breach occurring again. This might involve a step as simple as emailing all relevant members of our workforce to reinforce good practice, or providing additional training, or may in more serious cases require new technical systems and processes and procedures to be put in place.