IPSWICH HIGH SCHOOL

WOOLVERSTONE HALL

SUFFOLK, ENGLAND

Data Protection Policy

2023 – 2024

Data Protection Policy

Ipswich High School is a proprietorial school owned by Ipswich Education Limited (IEL), whose Board has the legal responsibility to ensure that all regulatory requirements are met. This means that the Proprietorial Board has a role that is different to many independent schools. It is the role of the Proprietorial Board to provide the school with strategic guidance and oversight. The Proprietorial Board, therefore, have powers of scrutiny and are enabled to make recommendations for change and improvement. The Proprietorial Board are supported by voluntary advisors who will offer their advice as a "critical friend". Board meetings are held every term.

Table of Contents

1. General Statement Of The Duties Of Ipswich High School

The Data Protection Act 1998 came into force on 1 March 2000. It is concerned with the rights of individuals to gain access to personal information held about them by an organisation or individual within it and the right to challenge the accuracy of data held. The terms of the Act relate to data held in any form, including written notes and records, not just to electronic data.

Ipswich High School is the data controller. The 'school' means Ipswich High School. This policy applies to personal information held and processed by Ipswich High School, and sets out its duties under the Data Protection Act 1998. It provides guidance on processing, retaining, security and disposal of all personal data held by Ipswich High School

Ipswich High School is required to process personal data regarding pupils, their parents or guardians and staff as part of their operation, and shall take all reasonable steps to do so in accordance with this Policy and the principles of the Data Protection Act 1998 ('the DPA').

The school aims to have transparent systems for holding and processing personal data. Any reference to personal data in this policy includes reference to sensitive personal data. Processing may include obtaining, recording, holding, disclosing, destroying or otherwise using data.

Any individual is entitled to request access to information relating to their personal data held on a relevant filing system by the school. A relevant filing system is any paper filing system or other manual filing system which is structured so that information about an individual is readily accessible. Personal data can be held in any format (electronic, paper-based, and photographic) from which the individual's data can be readily extracted

In this policy any reference to pupils includes current, past or prospective pupils.

2. The Data Protection Act 1998

Ipswich High School has the responsibility to comply with the DPA. The DPA applies to information relating to both "personal" and "sensitive personal" data.

Personal Data means data relating to a living individual who can be identified from that data. The school may process a wide range of personal data of pupils, their parents or guardians and staff, as part of their operation. To qualify as personal data, the data must allow you to identify and give information relating to a data subject. Personal data includes facts and any expression of opinion about an individual. Examples of personal data are: names and

addresses; bank details; academic, disciplinary, admissions and attendance records; references; and examination scripts and marks.

Sensitive personal data is defined in the DPA as information in respect of racial or ethnic origin, political opinions, religious beliefs or "other beliefs of a similar nature", membership of a trade union, physical or mental health, sexual life, criminal convictions and alleged offences. Sensitive personal data can only be processed under strict conditions, including a condition requiring consent of the person concerned to such processing.

In order to comply with the DPA the schools must comply with the eight Data Protection Principles which state that personal data must be:

Principle 1: Personal data will be processed fairly and lawfully.

The collection and disclosure of data is subject to scrutiny and is only 'lawful' if it meets at least one of the following criteria (as specified in Schedule 2 of the Act):

- With the consent of the data subject; or,
- In performance of a contract (for example to process an application as part of the admissions process); or,
- If there is a legal obligation (for example under prevention of terrorism legislation); or
- For the protection of the vital interests of the individual (for example to prevent injury or other damage to the health of the data subject), or,
- In the legitimate interest of the data controller, unless it is prejudicial to the interests of the individual (for example for the purpose of equal opportunities monitoring).

Personal Data must meet all of the following criteria in order to be processed 'fairly':

- Data will only be collected from persons who have the authority to disclose it. If personal information is collected from a third party, the data subject will be informed of the 'use' of the information.
- Subjects will not be deceived or misled in any matter related to the use of personal data.

In addition to the requirements outlined above, sensitive personal data may only be processed if it also meets at least one of the following criteria (as specified in Schedule 3 of the Act):

- The data subject has given explicit consent.
- It is necessary to meet requirements of employment law.
- It is necessary to protect the vital interests (i.e. if the situation is a matter of life or death) of the subject or another person.
- The data subject has already manifestly made the information public.
- It is necessary for legal proceedings, obtaining legal advice or defending legal rights.
- It is necessary for the carrying out of official or statutory functions.
- It is necessary for medical purposes.
- It is necessary for equal opportunities.
- It is necessary in order to comply with legislation from the Secretary of State.

Principle 2: Personal data will be obtained only for one or more specified and lawful purposes

Data will not be further processed in any manner incompatible with the initial specified purpose or those purposes for which it was obtained. To satisfy the first principle (fair processing) the data subject(s) must not have been misled or deceived as to the reason(s) for processing.

Principle 3: Data must be adequate, relevant and not excessive

Personal information, which is not necessary for the intended processing, must not be acquired, i.e. personal information cannot be collected just because 'it may be useful'.

Principle 4: Data must be accurate and up to date

Ipswich High School must ensure that there is a system in place to review data for accuracy and to ensure that it is up to date. Procedures must be in place to make any amendments requested by a data subject, or a record kept if the amendment is not considered appropriate.

Principle 5: Data must not be kept for longer than required for the purpose

Ipswich High School must indicate the length of time that data is to be in use and archived for any given purpose. This time period must be seen as justifiable for the particular purpose and in line with any legislation covering the processing.

Information should not be kept any longer than the time period indicated to the data subject. Ipswich High School must regularly review data held in order to assess whether information is still required. The Act recommends that Ipswich High School has a retention policy in place to ensure information is retained only for as long as is necessary.

The Data Protection Act recommends that Ipswich High School has a disposal policy in place to which all staff can refer when they need to dispose of personal information. A disposal record will assist Ipswich High School in responding to enquiries made under the Data Protection Act.

Before disposing of any data Ipswich High School will consider the following key points:

- Any legal requirements (e.g. possible negligence action).
- The length of any appeals procedure relating to the information.
- The number of times in the last two or three years that a particular type of record has been accessed.

Principle 6: Data must be processed in line with individual's rights

This is strongly linked to the first principle of fair and lawful processing. Data subjects have the right to know details of the processing and the right of access to personal information.

A data subject (including a member of staff) has the right to object to data processing relating to them which is likely to cause damage or distress to that data subject or another person. There are a number of provisos to this right, in particular:

- The damage or distress must result from unwarranted processing, or
- The data subject must not have given consent to the processing, or
- The processing is not necessary for the purposes of fulfilling a contract with the data subject; or for fulfilling a legal obligation of Ipswich High School, or for protecting the data subject's vital interests.

In addition the Act gives data subjects the right to object to processing used for the purpose of direct marketing and/or wholly automated decision making.

Data subjects have the right to have inaccurate data amended and to block future processing in cases of unlawful/unfair processing. Data Subjects must formally request their rights in writing and their rights are enforceable by the courts.

Principle 7: Data must be processed in a secure manner

Ipswich High School must guard against unauthorised and unlawful processing, e.g. access, alteration, disclosure or disposal. Appropriate security records must be kept in order to provide an audit trail. Personal information will, so far as possible, be:

- Kept in a locked filing cabinet; or
- In a locked drawer; or
- If it is computerised, be password protected; or
- Kept only on disk which itself is kept securely.
- Please also be aware that the school has an acceptable use policy for ICT, Mobile devices and social networking. This policy should be adhered to at all times. See Shared drive for policies.

When personal data is to be destroyed, paper or microfilm records will be disposed of by shredding or incineration; computer hard disks or floppy disks will be reformatted, over-written or degaussed.

Principle 8: Data shall not be transferred outside of the European Economic Area unless that country or territory ensures an adequate level of protection

If the Data is to be transferred to a country or territory that does not have adequate protection then at least one of the following conditions must be met:

- The data subject has given consent.
- It is necessary for the performance of a contract with the data subject.

- It is necessary for the performance of a contract that is in the interests of the data subject.
- The transfer is necessary for reasons of substantial public interest.
- The personal data is already on a public register.
- The transfer is necessary to pursue legal proceedings, legal advice or defending legal rights.
- It is in the vital interests of the data subject
- The Information Commissioner has approved the transfer on the grounds that it safeguards the rights and freedoms of the data subject.

3. Processing Personal Data

Processing of personal data includes obtaining, holding, recording, adding, deleting, augmenting, disclosing, destroying, printing or otherwise using data. Processing also includes transferring data to 3rd parties.

Consent may be required for the processing of personal data unless the processing is necessary for the school to undertake their obligations to pupils and their parents or guardians. Personal data, unless otherwise exempt from restrictions on processing under the DPA, will only be disclosed to third parties under the terms of this policy or otherwise with the consent of the appropriate individual.

The rights in relation to personal data set out under the DPA are those of the individual to whom the data relates. The school will, in most cases, rely on parental or guardian consent to process data relating to pupils, and those with 'parental responsibility' are entitled to receive relevant information concerning the child. A pupil of sufficient maturity and understanding has certain legal rights which the school must observe. These include the right to give or withhold consent and certain rights to confidentiality. In exceptional circumstances, if a conflict of interest arises between a parent and a pupil, the rights of, and duties owed to the Pupil will in most cases take precedence over those of the parent. (See Parent Contract)

4. Exemptions Which Allow Disclosure Of Personal Data To Third Parties

There are a number of exemptions in the DPA which allow disclosure of personal data to third parties, and the processing of personal data by the school and its employees, which would otherwise be prohibited under the DPA. The majority of these exemptions only allow disclosure and processing of personal data where specific conditions are met, namely:

a) the data subjects have given their consent;
b) to safeguard national security;
c) for the prevention or detection of crime;
d) to prevent serious harm to the data subject or a third party;
e) for the assessment of any tax or duty;
f) where it is necessary to exercise a right or obligation conferred or imposed by law upon the school (other than an obligation imposed by contract);

g) for the purpose of, or in connection with, legal proceedings (including prospective legal proceedings);
h) for the purpose of obtaining legal advice;

5. Responsibilities Under The Data Protection Act

Ipswich High School is the data controller under the DPA.

The Headteacher is responsible for the school's compliance with the Data Protection Act and ensuring that the school practices are consistent with this policy. The Headteacher or delegated responsibility to the Data Protection Officer is responsible for ensuring that all staff are aware of their responsibilities under the act and appropriate training is put in place.

6. Use Of Personal Data By The School

The DPA requires that the personal data held about pupils must only be used for specific purposes allowed by law. The school holds personal data on its pupils, including: contact details, assessment/examination results, attendance information, behaviour, both positive and negative and characteristics such as ethnic group, special educational needs, any relevant medical information, and photographs.

The data is used in order to support the education of the pupils, to monitor and report on their progress, to provide appropriate pastoral care, and to assess how well the school as a whole is doing, together with any other uses normally associated with this provision in an independent school environment.

The school may make use of limited personal data (such as contact details) relating to pupils, their parents or guardians for fundraising, marketing or promotional purposes and to maintain relationships with pupils of the school.

In particular, the school may:

a) Make available information to any internal association, society or club set up for the purpose of maintaining contact with pupils or for administration, fundraising, marketing or promotional purposes relating to the school, e.g. Alumni. The school will remain as data controller and this policy will govern data usage.
b) Make use of photographs of pupils in school publications and on the school website as set out in the parent contract.
c) Make personal data, including sensitive personal data, available to staff for planning curricular or extra-curricular activities;
d) Keep the pupil's previous school informed of his/her academic progress and achievements, e.g. sending a copy of the school reports for the pupil's first year at the school to his previous school.

Photographs with names identifying pupils will not be published on the school website, etc. without the express permission of the appropriate individual. This permission is gained through the completion and signature of the photography consent form.

Parents who do not want their child's photograph or image to appear in any of the school's promotional material, or be otherwise published, must also make sure their child knows this.

Pupils, parents and guardians should be aware that where photographs or other image recordings are taken by family members or friends for personal use, the DPA will not apply, e.g. where a parent takes a photograph of their child and some friends taking part in the school sports day. Parents or family members should seek permission to record events.

7. Disclosure Of Personal Data To Third Parties

The school may receive requests from third parties (i.e. those other than the data subject, the school, and employees of the school) to disclose personal data it holds about pupils, their parents or guardians. This information will not generally be disclosed unless one of the specific exemptions under the DPA which allow disclosure applies; or where necessary for the legitimate interests of the individual concerned or the school.

The following are the most usual reasons that the school may have for passing personal data to third parties. To:

a) give a confidential reference relating to a pupil;
b) give information relating to outstanding fees or payment history to any educational institution which it is proposed that the pupil may attend; Please note that the school reserves the right to share personal information with third party credit reference agencies if it is considered by the school to be necessary.
c) publish the results of public examinations or other achievements of pupils of the school;
d) disclose details of a pupil's medical condition where it is in the pupil's interests to do so, for example for medical advice, insurance purposes or to organisers of school trips;
e) provide information to another educational establishment to which a pupil is transferring;
f) provide information to the Examination Authority as part of the examinations process; and
g) provide the relevant information to the Government Department e.g. DfES, Ofsted, concerned with national education.

The Department for Education uses information about pupils for statistical purposes, to evaluate and develop education policy and to monitor the performance of the nation's education service as a whole. The statistics are used in such a way that individual pupils cannot be identified from them.

Any wish to limit or object to any use of personal data by third parties, except as stated above, should be notified to the Data Protection Coordinator in writing.

Where the school receives a disclosure request from a third party it will take reasonable steps to verify the identity of that third party before making any disclosure. When members of staff receive enquiries from third parties for personal data, the enquirer should be asked why the information is required. If

consent to the disclosure has not been given (and an exception does not apply) then the request should be declined. In normal circumstances information should not be disclosed over the phone to third parties. In most circumstances third parties should be asked to provide documentary evidence to support data requests.

8. Data Sharing Agreements With Third Party Organisations

Ipswich High School has third party agencies offering guidance and support services to pupils on a 1:1 basis. Examples of such services include the Independent Careers Service (ISCO), Connexions and various 'counselling' services. If such services operate on your school site, there are Data Protection and Confidentiality issues to consider.

In normal circumstances many services of this type offer a confidential service to pupils and will only share data with the school or parents with the consent of the pupil (age 12+) or in cases where an over-riding Duty of Care exists (e.g. if the pupil or someone else is in danger).

When such services are delivered on school premises, the school has the right to agree to the confidential nature of such a service or, alternatively, the school may insist that the service operates within the school policy on data handling. This latter approach places an expectation on the service to automatically keep the school informed of the content of sessions, held at the school, involving pupils.

Once the school has adopted a policy on the confidential nature or otherwise of such services, this policy should be made transparent to all parties concerned, including the 'service' the parents and the pupils. It is good practice to agree the approach to confidentiality from the outset to avoid incorrect assumptions being made by either party.

1. In the Service Level Agreement (SLA) with the agency, the school's expectation on confidentiality should be clearly stated. The SLA should require agency staff to make pupils aware of the confidential nature, or otherwise, of the service at the point of delivery, i.e. in the 1:1 session.

2. Parents should be made aware through newsletters, etc, of the type and nature of the services provided on site for transparency reasons. In normal circumstances parents should be informed if their son or daughter has an appointment with a service unless the school feels it would not be in the best interests of the pupil to do so. This approach reflects the agreement with parents in the parent contract. For example in the case of 'blanket' career interviews for all Year 11, a note in the newsletter informing parents that their son or daughter may be offered such an intervention this academic year, may suffice for transparency purposes. More sensitive 'counselling' interventions should be treated on a case by case basis taking into account the views of the pupil, if sufficiently mature.

9. Cloud Computing

Cloud hosted IT service needs to be discussed and agreed with the IT Manager before proceeding. It is likely a Service Level Agreement would be required with the provider.

10. Sharing Contact Lists With Parents

Some schools may wish to share lists of contact details with parents for use in emergencies, or to facilitate the smooth running of school trips, etc.

This sharing is not prohibited by the Data Protection Act. However, to do this the school must ensure that the following steps are taken to protect what may be sensitive and valuable contact lists.

1. The parents whose data is to be included on the list, must give explicit consent to inclusion.
2. The data items to be shared, e.g. name, address, email must be outlined.
3. The purpose for which the list can be used should be outlined in order to make it transparent to parents what they are consenting to. It is recognised that it is not possible to provide an exhaustive list of uses, however, examples of the types of uses envisaged, and prohibited will suffice.
4. Parents, when consenting to inclusion on the list, are also made aware of the need to keep the data safe while in their possession.

To help with this process, a template for collecting consent is available (Appendix). Please note that extra tick boxes may be added/deleted as required.

11. Accuracy Of Personal Data

The school will endeavour to ensure that all personal data held in relation to an individual is accurate. Individuals must notify the relevant school's Data Protection Coordinator in writing of any changes to information held about them. An individual has the right to request that inaccurate information about them is erased or corrected.

Schools will issue a Data Collection Sheet to all parents/guardians on an annual basis to help with data accuracy.

12. Security Of Personal Data

The school will take all reasonable steps to ensure that all personal information is held securely and is not accessible to unauthorised persons. Personal information will, so far as possible, be:

- Kept in a locked filing cabinet; or
- In a locked drawer; or
- If computerised, be password protected; or
- Kept only on disk which is itself kept securely.

All staff should be aware of the ICT Code of Conduct Policy which is separate to this document.

13. Rights Of Access By Data Subjects To Their Personal Data

Under the DPA, individuals have a right of access to their personal data held by the school. Generally in the case of pupils under the age of 12 years, the person with parental responsibility may exercise this right on their behalf. Pupils aged 12 years and over can exercise this right themselves or may authorise their parents to act on their behalf. The pupil's signature on the SAR form would be required in these circumstances. This is known as a "Subject Access Request". A request in writing will be accepted as long as satisfactory identification is given and the information request is clear, not excessive or vexatious. Where the pupil and parents are known to the school further identification will not be required. In other cases it is expected that picture I.D. such as passport or driving licence would be required.

Requests For Access To Records (Subject Access Requests)

A Subject Access Request (SAR) must be made in writing. A Subject Access Request Form (Appendix C) can be used for this purpose, or a letter from the Data Subject detailing the information required will suffice.

All requests for access to records must be noted on the relevant pupil's file.

The Data Protection Officer will oversee and ensure that the SAR is completed as outlined in this policy.

Responding To Requests For Access To Records

The school will send a written response to the applicant acknowledging receipt of the application form. This must be done within 5 days of the request being received by the school.

The school's Data Protection co-ordinator will manage the response to the applicant.

The Headteacher must authorise the applicant's request for access before any information is disclosed.

The school may also wish to get advice from the Solicitor in relation to a disclosure.

If the applicant's request for access is granted, the DPA requires such access to be given within one month of the request being received. The period does not begin until:

a) A request is received by the school.

b) the school has received sufficient information to enable it to identify the individual who is seeking access;

c) the school has received sufficient information to enable it to access the information requested.

Where the conditions set out above are fulfilled, in responding to the request, the school must give a description of the personal data that is being processed, the purposes for which the personal data is being processed, and the persons to whom the personal data are or may be disclosed.

The school must also provide, in an intelligible form, a copy of the information held and, where possible, details of the source of the information. Finally, where processing results in automated decision making which evaluates matters relating to the data subject (for example, in the marking of multiple choice questions), the data subject should be informed and advised of the logic involved in that decision-making.

Data subjects are not entitled to information where exemptions to the right of access apply (see below). Moreover, in these circumstances, the school must only give a notification to the data subject that no information has been identified which is required to be supplied under the DPA.

14. Exemptions To Access By Data Subjects

Confidential references given, or to be given by the school or Head, are exempt from access. The schools will therefore treat as exempt any reference given by them for the purpose of the education, training or employment, or prospective education, training or employment of any pupil or member of staff.

It should be noted that confidential references received from other parties may also be exempt from disclosure. However, such a reference can be disclosed if such disclosure will not identify the source of the reference or where, notwithstanding this, the referee has given their consent, or where disclosure is reasonable in all the circumstances.

Examination scripts, that is information recorded by pupils during an examination, are exempt from disclosure. However, any comments recorded

by the examiner in the margins of the script are not exempt even though they may not seem of much value without the script itself.

Examination marks do not fall within an exemption as such. However, the 40 day compliance period for responding to a request is extended in relation to examination marks to either five months from the day on which the school received the request (if all the necessary conditions are fulfilled), or 40 days from the announcement of the examination results, whichever is the earlier.

An exemption may also be considered in cases where a third party is identified and disclosure may be detrimental to that party.

Data covered by Legal Privilege is also exempt i.e. where it may be necessary to take legal advice regarding a Data Subject, this information is exempt from Subject Access Request.

15. Collection Of Data

All forms used by the school to collect personal data about a pupil will carry a standard Data Protection notice

Data subjects will be provided or guided to the Privacy Notices on the website which details how data is gathered, stored and retained and the purposes for which it may be used.

16. Retention Of Data

The school will not keep pupil and related data for longer than necessary. To this end records of Primary school pupil will be transferred securely to the next school. Any records or part of records retained will be disposed of 7 years after the pupil finishes their education at the school. Records of pupils in Secondary schools will be disposed of in line with D.O.B. + 25 years rule. Brief details will be retained on all pupils indefinitely for Alumni and PR purposes. These details will include: name of pupil, date of birth, address, telephone number, email address, name of parents, gender of pupil, year pupil joined the school, previous school, new school, joining date, leaving date, parents' occupations, year group on leaving. Exceptions to this include records where there may be ongoing litigation in which case the entire record will be retained until final disposition of the matter and thereafter for a period of 7 years.

Personal details of pupil applicants which did "not progress" will be disposed of after 2 years.

Staff records will be securely disposed of 7 years after a member of staff leaves Ipswich High School employment. Brief details will be retained on all staff indefinitely to satisfy future reference requests. These details will include full name, date of birth, job title, national insurance number and period of employment. Exceptions to this include records where there may be ongoing

litigation in which case the entire record will be retained until final disposition of the matter and thereafter for a period of 7 years.

Unsuccessful staff applications should be kept for 6 months after interview.

Accident books / logs relating to all accidents in school should be kept for 40 years after the accident has been recorded as a claim could be made up to that time. The accident book must meet HSE accident book requirements.

An Accident: is any unplanned or undesired event that results in injury to a person which requires significant first aid intervention.

A flagging process should also be maintained to identify those records which should not be deleted due to litigation or other reasons. The flagging process and accident log should be referred to prior to records being deleted to identify any exceptions.

17. Disposal Of Data

Please see Appendix J. Data Retention Guide.

18. Audit

An audit of the compliance with this policy will be carried out on an annual basis by the Data Protection Coordinator in the school. This audit will be coordinated by the Data Protection Officer for Ipswich High School (See Appendix D).
All schools must complete the Annual Data Protection Audit Return (Appendix O) at the start of each autumn term.

19. CCTV Code Of Practice

The Data Protection Act 1998 introduced a systematic legal control of CCTV surveillance through the publication of a Code of Practice that came into effect in March 2000. It was updated in July 2000 and again in October 2001.

Since that time it has become a criminal offence to use an un-notified, non-domestic CCTV system to observe or record people in a public or a private place. It is the responsibility of the Data Protection Officer to include CCTV in the schools DP Notification.

IHS must ensure that system in their school have signs that make the public aware that they are entering a zone which is covered by surveillance equipment. (Appendix E).

In addition, it is the responsibility of the Data Protection Coordinator in the school to ensure that procedures are agreed and in place with regard to day to day operation of the system (Appendix F).

A full copy of the Code is available on the Data Protection web site at http://www.ico.org.uk/for_organisations/data_protection/topic_guides/cctv

20. Access To Images

Access to images will be restricted to those staff who need to have access in accordance with the purposes of the system. A list of such staff may be obtained from the Data Protection Co-ordinator.

21. Access To Images By Third Parties

Disclosure of recorded material will only be made to third parties in strict accordance with the purposes of the system. Examples of third parties include enforcement agencies and tax authorities where images recorded would assist in a criminal or tax enquiry and the prevention of terrorism and disorder. In normal circumstances such agencies will supply appropriate paperwork supporting their request. For example a section 29.3 form will be supplied by the Police in normal circumstances. In emergencies where there is an imminent threat or danger appropriate paperwork may be supplied following limited disclosure.

All requests and subsequent actions will be logged including details of data released, completed request forms and timescales.

22. Access To Images By A Subject

- CCTV digital images, if they show a recognisable person, are personal data and are covered by the Data Protection Act. Anyone who believes that they have been filmed by CCTV. is entitled to ask for a copy of the data, subject to exemptions contained in the Act. **They do not have the right of instant access.**
- A person whose image has been recorded and retained and who wishes access to the data must apply in writing to the Data Protection co-ordinator. The Data Protection policy outlines the Subject Access Request process which should be followed. The Data Protection co-ordinator will respond to the request in line with the timescale contained in the policy and recognise the 40 day limit to provide the data if the request is granted.
- The Data Protection co-ordinator will then view the data and decide in conjunction with the Headteacher if access to the data and/or a copy will be provided to the applicant. If access to the specified data or a copy is to be provided a decision should also be made regarding the

need to seek consent or conceal the identity of other parties shown in the images if deemed necessary.

- The Data Protection Act gives the School the right to refuse a request for a copy of the data particularly where such access could prejudice the prevention or detection of crime or the apprehension or prosecution of offenders.
- If it is decided that a data subject access request is to be refused, the reasons will be fully documented and the data subject informed in writing, stating the reasons.

23. Publishing Examination Results

Publishing examination results is a common and accepted practice. The Act does not stop this happening. However, the Act does mean that the school have to act fairly when publishing results and where people have concerns about their or their child's information being published, schools must take those concerns seriously.

Fairness

The school should make sure that all pupils and their parents or guardians are aware as early as possible whether examination results will be made public and how this will be done. This information should be repeated at regular intervals, for example, at the start of each school year, or each examination term.

The school should also explain how the information will be published. For example, will results be listed alphabetically, or in grade order? Some pupils, parents and guardians might object if results are published in grade order.

Objections

In general, because a school has a legitimate interest in publishing examination results, pupils or their parents or guardians do not need to give their consent to publication. However, in a small number of cases publication may cause distress or harm. Objections should be considered before making a decision to publish. A school would need to have a justifiable reason to reject someone's objection to publication of their exam results.

24. Staff Data

The principles of the Data Protection act described in this policy also apply to staff data held in the school.

Staff are made aware of, and agree to their data being processed by Ipswich High School by signing their contract of employment.

Sensitive personal data will only be used by Ipswich High School for legitimate business, management and school purposes and will not be transferred to third parties without consent.

Staff data will be held securely in locked cabinets or password protected electronic formats.

Use of staff records will be limited to those personnel appointed by the Headteacher or Human Resources Manager as appropriate for specific purposes.

As with all data subjects, staff may request to see, or have a copy of their record under the Subject Access Request provision of the Data Protection Act. If a full copy of the record is requested, Ipswich High School has 30 days to respond fully if required.

Subject Access Requests should be made to the Data Protection Co-ordinator or using email headofcompliance@ipswichhighschool.co.uk

The exemptions listed earlier in this policy apply.

Staff records will normally be kept for 7 years after their employment has ceased. Unsuccessful applicants will have their data kept for 6 months after their application.

The Data Protection co-ordinator will address the retention periods in the annual audit. They will also remind appropriate staff of the requirement to dispose of expired data securely.

DBS checks are carried out routinely by Ipswich High School. Staff Records will only indicate whether a satisfactory or unsatisfactory check has been received. No additional details regarding the DBS check will be held on the staff record.

Appendix B: Roles & Responsibilities

Role of the Data Protection Officer

The role of the Data Protection Officer is to:

- Ensure that the organisation complies with the Data Protection Act 1998, and to ensure that employees are fully informed of their own responsibilities for acting within the law and that the public, including employees, are informed of their rights under the Act.
- Be the nominated officer in the Data Protection register maintained by the Information Commissioner, notify the fact of processing to the Information Commissioner and maintain the accuracy and currency of the organisation's notification
- Co-ordinate Data Protection Act activities (including training) and facilitate such user group meetings as necessary e.g. Data Protection Coordinator's group
- Ensure organisational compliance, and conformance with the Data Protection Principles
- Develop, implement and enforce a suitable and relevant Data Protection policy and ensure it is reviewed on an annual basis
- To undertake systematic Data Protection Act compliance audits in accordance with Information Commissioner's audit tool
- Assist with investigations into complaints about breaches of the Act and undertake reporting/remedial action as required.
- Co-ordinate Subject access requests.
- Maintain and update own knowledge of developments in Data Protection issues.
- Be a resource for other employees by providing expert advice on the Data Protection Act and related issues.

Role of the Headteacher

The Headteacher is responsible for the successful implementation of this policy in their school. The Headteacher will agree and authorise all data to be released in connection with a S.A.R. (Subject Access Request).

Appendix C: Subject Access Request Form

Request for information under the Data Protection Act 1998

This form should be completed only if you are requesting personal information relating to yourself or on behalf of a third party.

Please complete in block capitals or type. *(* Required Fields)*.

1. Personal details of the person requesting the information.

Surname:	
Forename:	
Address:	
Postcode:	
Telephone number:	
Email:	

2. Are you the Data Subject *(i.e. the person whose information you are requesting)?* Please tick the appropriate box.

Yes □ *(Please go straight to question 5)*

No □

3. Personal details of the Data Subject *(if different from those at section 1)*.

Surname:	
Forename:	
Address:	
Postcode:	
Date of birth:	
School attended:	
Telephone number:	
Email:	

4. Please describe your relationship with the Data Subject that leads you to make this request on their behalf.

---

5. Information requested

If you would like to see only specific document(s), please describe these below.

---

6. If you would like a full copy of the personal records held by the school, please tick here □.

Declaration
I certify that the information given in this application form to the school is true. I understand that it will be necessary for the school to confirm my/the Data Subject's identity and it may be necessary to supply more detailed information if required.

Signature (Parental Responsibility) ----------

Print Name ----------

Date ----------

Signature (Pupil 12+) ----------

Data Protection Act 1998
The Data Controller is Ipswich High School. The details you provide on this form will only be used in connection with your application for the supply of documents and for statistical purposes.

The completed form should be returned to:

Head of Compliance – Data Protection
Ipswich High School
Woolverstone
Ipswich
Suffolk IP9 1AZ

I understand that I will receive acknowledgement of my request within 5 days of receipt. My request will be completed within 40 days in normal circumstances in accordance with the DP Act. However please note that Ipswich High School will endeavour to complete your request as soon as is practical within this 40 day period

Office use only

Received by:	Date:

Forwarded to:	Date:
Date to be completed by:	
Comments:	

Appendix D: Audit Outline

1. Aims of Data Protection Compliance Audits

- Mechanisms for ensuring that information is obtained and processed fairly, lawfully and on a proper basis.
- Quality Assurance, ensuring that information is accurate, complete and up-to-date, adequate, relevant and not excessive.
- Retention, appropriate weeding and deletion of information.
- Documentation on authorised use of systems, e.g. codes of practice, guidelines, etc.
- Compliance with individual's rights, such as subject access.
- To assess the level of compliance with the organisation's own data protection system.
- To identify potential gaps and weaknesses in the data protection system.
- To provide information for data protection system review.

2. Audit Objectives

When carrying out a Data Protection Audit in any area of an organisation the Auditor has three clear objectives:

I. To verify that there is a formal (i.e. documented and up-to-date) data protection system in place in the area.
II. To verify that all the staff in the area involved in data protection:
    a. Are aware of the existence of the data protection system;
    b. Understand the data protection system;
    c. Use the data protection system.
III. To verify that the data protection system in the area actually works and is effective.

3. Areas to be examined include:

- Use of appropriate forms when collecting data.
- Storage of data in accordance with the security policy, e.g. locked cabinets, passwords, etc.
- Data being removed in accordance with policy timescales.
- Subject Access Request process in place.
- CCTV compliance. Checklist completed and sent to the Data Protection Officer.
- Staff training requirements assessed and highlighted.

Appendix E. CCTV Signage Advice

All signs should be clearly visible and legible to members of the public. The size of signs will vary according to circumstances. For example:

- A sign on the entrance door to a building office may only need to be A4 size because it is at eye level of those entering the premises.
- Signs at the entrances of car parks alerting drivers to the fact that the car park is covered by such equipment will usually need to be large (probably A3 size) as they are likely to be viewed from further away, e.g. by a driver sitting in a car.

The signs should contain the following information:

- Identity of the person or organisation responsible for the scheme.
- The purposes of the scheme.
- Details of whom to contact regarding the scheme.

Appendix F: CCTV Operational Checklist

Introduction

This checklist is designed to help operators of small CCTV systems comply with the legal requirements of the Data Protection Act 1998 and it details the main issues that need to be addressed when operating a CCTV system. When used as part of a regular review process it should help to ensure that the CCTV system remains compliant with the requirements of the Act.

It is important that the Data Protection Act is complied with because failure to do so may result in action being taken under this Act. Failure to comply with Data Protection requirements will also affect the police's ability to use the CCTV images to investigate a crime and may hamper the prosecution of offenders.

If you use a CCTV system in connection with your school you should work through the checklist and address all the points listed. This will help to ensure that your CCTV system remains within the law and that images can be used by the police to investigate crime.

Small User Checklist
Operation of the CCTV System

This CCTV equipment and the images recorded by it are controlled by …….. who is responsible for how the system is used and for the notifying the Information Commissioner about the CCTV system and its purpose (this is a legal requirement of the Data Protection Act 1998).

The above controller has considered the need for using a CCTV system and has decided it is required for the prevention and detection of crime, for protecting the safety of customers and for the general running of the school. It will not be used for other purposes.

Description	Checked (Date)	By	Date of next review
The controller is aware that notification to the Information Commissioner is necessary and must be renewed annually.			
Notification has been submitted to the Information Commissioner and the next renewal date recorded .			
Cameras have been sited so that their images are clear enough to allow the police to use them to investigate a crime.			

Description	Checked (Date)	By	Date of next review
Cameras have been positioned to avoid capturing the images of persons not visiting the premises.			
There are signs showing that a CCTV system is in operation visible to people visiting the premises and the controllers contact details are displayed on the sign where it is not obvious who is responsible for the system.			
The recorded images from this CCTV system are securely stored, where only a limited number of authorised persons may have access to them.			
The recorded images will only be retained for 14 days to allow any incident to come to light (e.g. for a theft to be noticed).			
Recordings will only be made available to law enforcement agencies involved in the prevention and detection of crime, and no other third parties.			
The operating equipment is regularly checked to ensure that it is working properly (e.g. the recording media used is of an appropriate standard and that features on the equipment such as the date and time stamp are correctly set).			
The controller knows how to respond to requests from individuals for access to images relating to that individual. See CCTV Code of Practice.			

Appendix J: Data Retention Guide

1. Purpose of the Data Retention Guide

In the course of its activities every school creates and receives a large amount of information. Much of this information contains personal data which is in turn subject to the Data Protection Act 1998 (DPA).

Personal data is any information relating to a living individual and would include information on pupils, members of staff and other employees. Data is very widely construed and can include internal files, letters, faxes, memoranda and notes, email, computer data and even voicemail, SMS and CCTV images created or received in the course of your operations.

It is extremely important that data is held for the correct period of time so as to be available for the proper needs of the school. Indeed some classes of data are required by law or good business practice to be kept for a specified period of time and failure to do so may at best prejudice the position of the school and at worst expose the school or its staff and employees to potential lawsuits and/or fines or even put them in contempt of court. However, keeping all data for an unlimited period of time will not only be impractical but will also expose the school to risk under the DPA. This is because the retention of unnecessary data will create a compliance risk under the DPA as this requires that personal data is:

- Adequate relevant and not excessive;
- Accurate and up to date;
- Not kept for longer than is necessary

The excessive storage of data is not only highly obstructive to the smooth operation of the school but will also create a risk of prejudicing some or all of the above data protection principles.

The purpose of this guide is to provide guidelines for the retention, storage and disposal of the data held by the school.

2. Retention Periods

Except as otherwise indicated in accordance with paragraph 4 below data should be retained for the number of years indicated in the Retention Schedule below.

The school is responsible for the implementation of this guide.

Where, in accordance with paragraph 4, it is necessary for a school to retain certain data for a period beyond the period indicated in the schedule, the school will maintain a flagging process to identify those records which must be retained beyond the specified period. The flagging process employed will be dictated by the records system in use.

Unless a flag has been given in respect of specific data then data should be destroyed as soon as practicable after expiry of the specified retention period.

3. Disposal of Records

A document which is to be destroyed in accordance with this guide is likely still to be sensitive in the wrong hands, to deal with confidential or personal matters and/or have other security implications. The method by which these types of documents are disposed is of importance both because of the inherent risk such material falling into the wrong hands and because in accordance with Principle 7 of the DPA, the school has a legal duty to ensure that it is disposed of securely. The method of disposal of data shall be consistent with the type of data being destroyed. Confidential data should be disposed of in a way that prevents the data from being accessible to others.

The main disposal methods and safeguards are as follows:

- Secure destruction and recycling by specialised firms. The security of the service provider's methods should be fully investigated and guarantees built into any contract where possible.
- Shredding. For highly sensitive documents some types of shredding may not be sufficient and the waste may itself need to be destroyed in order to ensure that it cannot be pieced back together (this would be far more difficult if a quality cross-cut shredder was used). If shredding is done centrally, consideration may need to be given to the security of documents awaiting destruction.
- Incineration. Consideration will need to be given to environmental and other safety implications.
- Overwriting electronic data, or otherwise making it unreadable. Care needs to be taken to ensure that sensitive data is completely erased. For example, deleting a file on a PC may only delete the file reference and not the underlying data. With the right tools and knowledge, it is possible to reconstruct the file. Great care should also be taken to ensure the secure disposal of physical IT equipment upon which the personal data may have been held or processed.

4. Archiving data

In general, once data or documents are no longer "live" they should be moved to archiving as soon as is reasonably possible. Archiving should not be confused with destruction. You need to keep in mind that archived data and documents carry with them on-going obligations and are subject to the requirements of the DPA, for instance, archived data and documents will need to be considered in the event of any subject access request and the archiving system must be kept properly secure.

Data and documents which have been archived should be reviewed against the criteria set out in this guide with a view to destruction after the relevant time period. Ultimately the archival period for data and documents is a matter of balancing costs of holding the data or

documentation in archive which is highly unlikely ever to be needed against the general principle that everything else being equal, and it is better to be safe than sorry.

5. Retention of Data beyond the Retention Period

Where data should be retained indefinitely:-

(1) If you receive notice of any lawsuit, government or regulatory investigation (for instance, health & safety investigations), other legal action, complaint or claim against or involving the school, the School or any member of staff, or employee, or pupil or any of circumstances likely to give rise to such an action, proceeding, investigation complaint or claim, then you should flag all data which may be relevant for preservation in respect of the same. Any data so flagged shall be preserved and shall not be destroyed

(2) If any member of staff or employee becomes aware that any notice has been received by the school of any lawsuit, government or regulatory investigation, other legal action, complaint or claim against or involving Co, the school or any member of staff, employee or pupil or any of circumstances likely to give rise to such an action, proceeding, investigation, complaint or claim, that member of staff or employee should immediately notify the school's Data Co-ordinator in order that the Co-ordinator can review which data should be [flagged] for extended retention in accordance with this guide. The member of staff or employee must not destroy any data relevant to such action, proceeding, investigation, complaint or claim whether it not it would otherwise fall to be destroyed in accordance with this guide.

(3) If any member of staff or employee is unsure whether any unflagged data is relevant to an action, proceeding, investigation complaint or claim the member of staff or employee should not delete that data and should liaise with Data Co-ordinator.

Once data has been flagged all members of staff and employees must preserve and prevent the destruction of any such data (including e-mails and other computer records).

Destruction of such data, even if inadvertent, could seriously prejudice the member of staff or employee and the school and could subject the individual, or the school to substantial criminal and civil liability including fines and other penalties.

Whenever data is flagged the data shall be preserved until the flag is removed. The communication imposing the [flag] shall be stored with the preserved data until that flag is removed, following which the data shall be destroyed as soon as reasonably possible.

6. Violations

Due to the potentially serious consequences of a violation of the procedures set out in this guide any violation may be subject to disciplinary action.

All members of staff or employees should report any suspected violations of this guide to the Data Protection Officer.

7. Questions

Anyone with questions about this guide should contact their Data Protection Co-ordinator or the *Data Protection Officer*.

DATA RETENTION SCHEDULE

1. Child Protection			
Basic File Description	**Statutory Provisions**	**Retention Period**	**Notes & Actions**
1.1 Child Protection files	Education Act 2002, s175, related guidance "Safeguarding Children in Education", - September 2004	D.O.B. +25 years	SECURE DISPOSAL unless legal action is pending
1.2 Allegation of a child protection nature against a member of staff, including where the allegation is unfounded.	Employment Practices Code: Supplementary Guidance 2.13.1. (Records of Disciplinary and Grievance) Education Act 2002 guidance "dealing with Allegations of Abuse against Teachers and Other Staff" November 2005	Until the person's normal retirement age or 10 years from the date of the allegation whichever is the longer.	SECURE DISPOSAL unless legal action is pending

2. Employer Policies, Personnel Records, and Payroll Documents			
Basic File Description	**Statutory Provisions**	**Retention Period**	**Notes &Actions**
2.1 Records related to the formulation of HR Policies and an Employee Handbook		Permanent	SECURE DISPOSAL unless legal action is pending
2.2 List of all members of staff and employees and dates of employment		7 years after termination of employment	SECURE DISPOSAL unless legal action is pending

2. Employer Policies, Personnel Records, and Payroll Documents			
Basic File Description	**Statutory Provisions**	**Retention Period**	**Notes &Actions**
2.3 Employee offer letters, confirmation of employment letters, written particulars of employment , contracts of employment and changes to the terms and conditions		7 years after termination of employment	SECURE DISPOSAL unless legal action is pending
2.4 Information on benefits per member of staff/employee		7 years after termination of employment	SECURE DISPOSAL unless legal action is pending
2.5 Pension records		7 years after termination of employment	SECURE DISPOSAL unless legal action is pending
2.6 Training records		7 years after termination of employment	SECURE DISPOSAL unless legal action is pending
2.7 Collective workforce agreements and works council minutes		Permanently	SECURE DISPOSAL unless legal action is pending
2.8 Job applications, CVs and interview records	The Information Commissioner's Employment Practices Code, Parts 1.7.5 and 1.7.6	6 months after notifying unsuccessful candidates; 7 years after termination of an employee if the applicant *is* hired	SECURE DISPOSAL unless legal action is pending
2.9 Personnel Files (including all records relating to promotions, demotions, grievance procedures, resignation or termination letters)		7 years after termination of employment	SECURE DISPOSAL unless legal action is pending
2.10 Disciplinary Matters			
2.10.1 Verbal Warning	Employment Relations Act 1998	Records resulting from a verbal warning should be	SECURE DISPOSAL unless legal action is pending

2. Employer Policies, Personnel Records, and Payroll Documents			
Basic File Description	**Statutory Provisions**	**Retention Period**	**Notes &Actions**
		retained on file for 6 months then destroyed.	
2.10.2 Written Warning	Employment Relations Act 1998	Records resulting from a written warning should be retained on file for 12 months then destroyed.	SECURE DISPOSAL unless legal action is pending
2.10.3 Final Written Warning	Employment Relations Act 1998	Records resulting from a final written warning should be retained on file for 12 months then destroyed.	SECURE DISPOSAL unless legal action is pending
2.11 Job descriptions and performance goals		7 years after termination of employment	SECURE DISPOSAL unless legal action is pending
2.12 Immigration checks	Immigration, Asylum and Nationality Act 2006	Up to 2 years after termination of employment	SECURE DISPOSAL unless legal action is pending
2.13 Records in relation to hours worked and payments made to workers	Section 9, National Minimum Wage Act 1998 Regulation 38, National Minimum Wage Regulations 1999	3 years beginning with the day upon which the pay reference period immediately following that which they relate ends	SECURE DISPOSAL unless legal action is pending
2.14 Records relating to accidents / injury at work.		Date of incident +40 years	SECURE DISPOSAL unless legal action is pending

2. Employer Policies, Personnel Records, and Payroll Documents			
Basic File Description	**Statutory Provisions**	**Retention Period**	**Notes &Actions**
2.15 Information relating to the member of staff's/employee's exposure to toxic substances (Medical Records to be stored separately in confidential location.)		Permanently	SECURE DISPOSAL unless legal action is pending
2.16 Working time opt-out forms	Regulations 5 and 9, Working Time Regulations 1998	2 years from the date on which they were entered into.	SECURE DISPOSAL unless legal action is pending
2.17 Records to show compliance with the Working Time Regulations 1998	Regulations 5, 7 and 9, Working Time Regulations 1998	2 years after the relevant period.	SECURE DISPOSAL unless legal action is pending
2.18 Annual leave records		6 years or possibly longer if leave can be carried over from year to year.	SECURE DISPOSAL unless legal action is pending
2.19 Payroll and wage records for companies		6 years from the financial year end in which payments were made.	SECURE DISPOSAL unless legal action is pending
2.20 Maternity records	Regulation 26, Statutory Maternity Pay (General) Regulations 1986	3 years after the end of the tax year in which the maternity pay period ends.	SECURE DISPOSAL unless legal action is pending
2.21 Current bank details		No longer than necessary.	SECURE DISPOSAL unless legal action is pending

2. Employer Policies, Personnel Records, and Payroll Documents			
Basic File Description	**Statutory Provisions**	**Retention Period**	**Notes &Actions**
2.22 Records of advances for season tickets and loans		While employment continues and up to 6 years after repayment.	SECURE DISPOSAL unless legal action is pending
2.23 Death benefit nomination and revocation forms		While employment continues or up to 6 years after payment of benefit.	SECURE DISPOSAL unless legal action is pending
2.24 Consents for the processing of personal and sensitive data		For as long as the data is being processed and up to 6 years afterwards	SECURE DISPOSAL unless legal action is pending
2.25 Disclosure and Barring Service checks and disclosures of criminal record forms	Rehabilitation of Offenders Act 1974 The Information Commissioner's Employment Practices Code, Parts 1.7.4 and 2.15.3	Should be deleted following recruitment process unless assessed as relevant to ongoing employment relationship. The information may include information on any spent conviction permitted under the exceptions order	SECURE DISPOSAL unless legal action is pending
2.26 Emails - School based staff		Mail is retained for 6 months after a member of staff leaves employment.	SECURE DISPOSAL unless legal action is pending

2. Employer Policies, Personnel Records, and Payroll Documents			
Basic File Description	**Statutory Provisions**	**Retention Period**	**Notes &Actions**
2.27 Emails - Head Office staff		Mail is retained for 10 years after a member of staff leaves employment.	SECURE DISPOSAL unless legal action is pending
2.28 My Documents		Retention is down to local school policy	SECURE DISPOSAL unless legal action is pending

3. Pupil records			
Basic File Description	**Statutory Provisions**	**Retention Period**	**Notes & Actions**
3.1 Admission Registers		Date of last entry in the book (or file) +7 years.	SECURE DISPOSAL unless legal action is pending
3.2 Attendance Reports		Date of register + 3 years	SECURE DISPOSAL unless legal action is pending
3.3 Pupil Files Retained in Schools			
3.3.1 Primary		Transfer pupil files to the next school when the child leaves. All data except Alumni to be removed 7 years after pupil has left school	SECURE DISPOSAL unless legal action is pending
3.3.2 Secondary	Limitation Act 1980	D.O.B. of pupil + 25 years	SECURE DISPOSAL unless legal action is pending
3.3.3 Pupil applicants who did not enrol		2 years after application	SECURE DISPOSAL unless legal action is pending

3. Pupil records			
Basic File Description	**Statutory Provisions**	**Retention Period**	**Notes & Actions**
3.3.4 Special Educational Needs files, reviews and Individual Education Plans		D.O.B. of the pupil + 35 years the review. NOTE; This retention period is the minimum period that any pupil file should be kept.	SECURE DISPOSAL unless legal action is pending
3.3.5. Records relating to accidents / injury in school		Date of incident +40 years.	SECURE DISPOSAL unless legal action is pending
3.4 Examination Results			
3.4.1 Internal examination results		7 years after leaving school	SECURE DISPOSAL unless legal action is pending
3.4.2 Any other records created in the course of contact with pupils		7 years after leaving school	SECURE DISPOSAL unless legal action is pending
3.4.3 Statement maintained under the Education Act 1996 section 324.	Special Education Needs Disability Act 2001 section 1.	D.O.B. + 35 years	SECURE DISPOSAL unless legal action is pending
3.5 Proposed statement or amended statement	Special Education Needs Disability Act 2001 section 1.	D.O.B. + 35 years	SECURE DISPOSAL unless legal action is pending
3.6 Advice and information for parents regarding Educational needs	Special Education Needs Disability Act 2001 section 2.	Closure + 12 years	SECURE DISPOSAL unless legal action is pending

3. Pupil records			
Basic File Description	**Statutory Provisions**	**Retention Period**	**Notes & Actions**
3.7 Accessibility strategy	Special Education Needs Disability Act 2001 section 14.	Closure + 12 years	SECURE DISPOSAL unless legal action is pending
3.8 Parental permission slips for school trips where there has been no major incident.		Conclusion of trip	SECURE DISPOSAL unless legal action is pending
3.9 Parental permission slips for school trips where there has been a major incident	Limitation Act 1980	D.O.B. of the pupil involved in the incident + 25 years. The permission slips for all pupils on the trip need to be maintained to show that the rules for all pupils had been followed.	SECURE DISPOSAL unless legal action is pending
3.10 Pupil emails		Retention is down to local school policy	SECURE DISPOSAL unless legal action is pending
3.11 My Documents		Retention is down to local school policy	SECURE DISPOSAL unless legal action is pending

4. Complaint Records			
Basic File Description	**Statutory Provisions**	**Retention Period**	**Notes & Actions**

4.1 Any data relating to a complaint, issue or potential complaint or issue relating to - any pupil: - the school - any act or omission of any member of staff or other employee or any contractor engaged by the school: - anything which happened in or around any premises occupied by the school		During the period which the complaint or issue is investigated until final disposition of the matter and thereafter for a period of 7 years . **DO NOT DESTROY OR DELETE UNLESS AND UNTIL DESTRUCTION HAS BEEN SPECIFICALLY APPROVED BY HEADTEACHER AND DATA PROTECTION OFFICER**	Please refer to IHS Complaints Procedure Policy
4.2 Other e-mail any attachments and voice recording (**unless** other provisions of this guide apply requiring longer retention)		For the period of 2 years	Note : Subject to any, longer retention period which may be required under other provisions of this guide

5. Litigation			
Basic File Description	**Statutory Provisions**	**Retention Period**	**Notes & Actions**

5.1 Records relating to pending, threatened or reasonably anticipated litigation, government investigation, or complaint or other claim		During the period in which the litigation, investigation complaint or claim is contemplated, pending or threatened and until final disposition of the matter and thereafter for a period of 7 years .**CHECK WITH HEADTEACHER AND DATA PROTECTION OFFICER BEFORE DESTROYING**	SECURE DISPOSAL unless legal action is pending

Appendix J1: Disposal Log

DATE	DESCRIPTION	RECORDS INCLUDED	EXCEPTIONS
	Example: Annual audit of records in line with retention timescale or request from subject to change or delete record.	Records reaching D.O.B. + 25 years rule.	Individual pupils record as per retention log e.g. for legal proceedings ongoing etc.

Appendix K1: S.A.R. Process Sheet

SAR reference:					
Date Acknowledged					
Target Date to DPA					
Target Date for Release					
Verification of Subject					
Date:	**Description of document; letter / email / report inc who from / to and 'cc' details.**	**Editing done and reasons given. E.g. Third parties anonymised.**	**Notes – check names for editing.**	**Copies Taken**	**Signature**
Correspondence (sections within the file are noted)					
Emails					
Sims					
Minutes of meetings					
Notes of visits					
Student File					
CCTV					
Accident Book					
Staff Personal File					
Sickness Records					
Other (Specify)					
Signature of DPA					
Date					

Appendix K2: S.A.R. Release Letter

[Name]
[Address]

[Date]

Dear [Name of data subject]

Data Protection Act 1998: Subject Access Request

Thank you for your correspondence of [date] making a data subject access request for [subject].

We are pleased to enclose the information you requested.

We have endeavoured to provide all the information that we hold on the data subject. However, if you have any reason to believe that there is any missing data then please do not hesitate to seek further clarity from us on this matter.

Yours Sincerely

Appendix L: Parents Contact List Consent Form

Ipswich High School would like to circulate a list to enable parents to contact each other regarding legitimate school activities, e.g. school trips, emergency closures, sports day.

In order to include your details on this list we require your explicit consent. If you are happy to be included please fill out the appropriate details below, sign and return to <named individual>.

Parental Consent

I agree to have the following details included on the contact list which will be distributed among parents of <XYZ> School, to support legitimate school activities.

Please tick.

Name:	☐
Address:	☐
Mobile number:	☐

In addition, I recognise that this data, when in my possession is only to be used for legitimate school activities. Examples of these activities are included above. The above list is not exhaustive. I recognise that I must not use the data in connection with any commercial activity or to promote any club, user group, and society or charity organisations. I will not pass this data onto any third parties. If in doubt I will contact the school to clarify.

The data on the list is sensitive and potentially valuable and I undertake to keep it secure when in my possession.

I understand that consent information will be kept on file for the duration of my child's time at school. If I wish to withdraw this consent I will write to the school to request this.

Signed:

Name (please print):

Date:

Sufficient maturity*

The Information Commissioner would regard a young person age 12 to be of sufficient maturity to exercise their rights under the Data Protection Act. This

includes the right to Consent or withhold consent to share. This is a general guide and it is recognised that some younger people may be sufficiently mature whereas some older people may not.

Appendix O: Data Protection Audit Return

School / Site Name:
Year:

Ref	Description	Current Situation	Status	Action(s)	Owner	Deadline
1.0	**Staff / Pupil Records**					
1.1	Student data is kept in accordance with the data retention policy.					
1.2	Staff data is kept in accordance with the data retention policy.					
1.3	Expired records are disposed of safely and securely by named individuals.					
1.4	All forms used to collect data are identified.					
1.5	All forms used to collect data include the standard Data Protection disclaimer.					
1.6	The Pupil Data Collection sheet (Appendix G) is sent out to parents, annually at a set time, to collect/refresh pupil data.					
1.7	All electronic databases in use, including the users who can access them, are identified.					
1.8	Access to all electronic databases is secured by individual					

Ref	Description	Current Situation	Status	Action(s)	Owner	Deadline
	username and password.					
1.9	All paper record systems in use, for staff or pupils, are identified.					
1.10	All paper record systems are secured in accordance with policy guidelines.					
1.11	Staff with access to staff records is documented, controlled and regularly reviewed.					
1.12	The standard Parent Contract is being used.					
1.13	The Accident Book is used for pupils and records are kept for 40 years from the date the incident is logged.					
1.14	The Accident Book is used for staff and records are kept for 40 years from the date the incident is logged.					
1.15	All pupils, whose parents have opted not to have their photograph used, are clearly identified with the information easily accessible to staff.					
2.0	**Procedures**					
2.1	All third party organisations offering a service on your premises, including the data they collect (if any), are identified. Are any 3rd party provider using					

Ref	Description	Current Situation	Status	Action(s)	Owner	Deadline
	Cloud based services, if so please confirm you have discussed this with the Head of IT as indicated in the policy.					
2.2	All Service Level Agreements with third party organisations are reviewed to consider data handling compliance.					
2.3	All CCTV systems installed at your premises (if any) are documented.					
2.4	Appropriate CCTV signage is in place?					
2.5	The CCTV checklist (Appendix F) is completed annually and returned to the Data Protection Officer					
2.6	The school has a policy in place regarding the use of photography/video by family members at events. The method and frequency of communicating this to parents is documented and completed.					
2.7	Contact details of parents are not distributed to other parents, for legitimate school activities, unless a					

Ref	Description	Current Situation	Status	Action(s)	Owner	Deadline
	signed Parent Consent Form is received by the school (Appendix L).					
2.8	A Subject Access Request (SAR) file is in place to store requests.					
2.9	The SAR process has been tested. Please complete Appendix K1 for a random pupil to test the process and outline any issues or concerns.					
3.0	**Staff Training**					
3.1	Staff are made aware of the school's Data Protection policy and its implications for them in their work.					
3.2	Staff are made aware of the school's ICT policy, mobile devices and social networking sites policy and its implications for them in their work.					
3.3	Staff are made aware of that they must inform the school of any changes to their personal details, e.g. change of address, contact numbers.					

Ref	Description	Current Situation	Status	Action(s)	Owner	Deadline
3.4	Have you received staff DP training materials?					
3.5	Have all staff had the minimum training session and been given the DO & DON'T LIST? If not when is this planned? *(Expectation is that all staff will have been trained by Christmas 2014).*					

Status Key:

Status	Description
	Policy standard not met.
	Policy standard partially met. Action Plan in place to achieve full compliance.
	Policy standard achieved.

Audit completed by (please print):

Signed:

Position:

Date:

Appendix P: Data Safety

Remember:

Data we record about individuals (staff, pupils, parents etc) is covered by the Data Protection Act and belongs to that individual. As such, notes we make on SIMS, PORTAL, in emails and paper records may be seen by the person

concerned.

We have access to data as part of our role within the school. This data should not be disclosed or used for any purpose that is not official business of the school.

The school has a data protection co-ordinator who can provide advice in case of uncertainty.

Here is a list of 'top tips' when handling school data.....

DO ☑

- Record facts and professional opinions only, on school records, emails and other similar documents
- Use a strong password on I.T. Systems at work, e.g. a combination of 8 or more alphanumeric characters and symbols.
- Change passwords on a regular basis.
- Password protect email attachments containing personal or commercially sensitive data.
- Encrypt any removable data devices including USB sticks laptops and similar.
- Remember the school may incur substantial fines for loss or misuse of data.
- Read and familiarise yourself with the IT Policy.
- Keep data secure when using it off site.
- Think security when posting sensitive documents.

DON'T ☒

- Use personal social media with pupils.
- Contact pupils or store pupil/parent contact data on personal devices, e.g. numbers on your mobile.
- Use your mobile phone outside designated areas in school.

- Don't share passwords.
- Don't leave personal data unattended when off site.
- Don't create databases of Personal Data in addition to the official sources e.g. SIMS and PORTAL.

Taking Data Off Site

- Only take offsite, information you are authorised to and only when it is necessary.
- ensure that it is protected offsite by not leaving it unattended,
- locking it away when not in use,
- not discussing or sharing it with non-school staff.
- be aware of your location and take appropriate action to reduce the risk of theft
- make sure you sign out completely from any online services you have used e.g. email
- try to avoid other people seeing the information you are working with
- treat records as if they were your bank details and PIN

Key Contacts

Author	Nicola Griffiths
Role	Deputy Head
Date Written	August 2018
Date updated	August 2019
Minor updates	March 2020
Reviewed By	Elizabeth Hill Oct 2023
Next Review Date	August 2024