Data Policies

Shrewsbury School is committed to fulfilling its obligations as a "Data Controller" under the GDPR/Data Protection Act. The table in appendix A provides an organisation structure of the data management responsibilities within the school.

- The Audit sub-committee is tasked with oversight of the data management controls.
- The Bursar is the "Privacy and Compliance Officer" and is the primary contact for questions about compliance with data protection law, reporting of data breaches and fulfilling subject access and other statutory requests, and ensuring that staff receive appropriate training when handling personal data. In this role he reports into the Audit Committee each March, and reports at least termly to the IT Steering Group. Questions on Packwood should be directed to the Packwood Bursar in the first instance
- The IT Steering Group – This group, comprising the Bursar, Senior Master, Deputy Head Academic, Deputy Head Co-curricular, Deputy Head Pastoral, Director of IT Services and two other members of Common Room, meets twice a term. This group will receive reports on data protection and data security issues from the Privacy and Compliance Officer and the Data Security Officer, and will assess data protection risks, and keep a register available for inspection by the Audit Committee.

The school has the following policies as part of its Information Governance Management Framework:

- Privacy Notice (Appendix B & separately on website)
- Data storage retention guidelines (Appendix C)
- Data breach guidance (Appendix D)
- Taking, storing and using images of children policy (Appendix E)
- CCTV Policy (Appendix F)
- Data security policies (Held by Director of IT Services)
- Non Pupil Acceptable Use Policy
- Pupil Acceptable Use Policy

The following policies also refer to data protection:

- Safeguarding
- Staff Code of Conduct
- Whistle-blowing Policy
- Other IT policies (Social Media, Cyber-bullying, Device for learning policy)

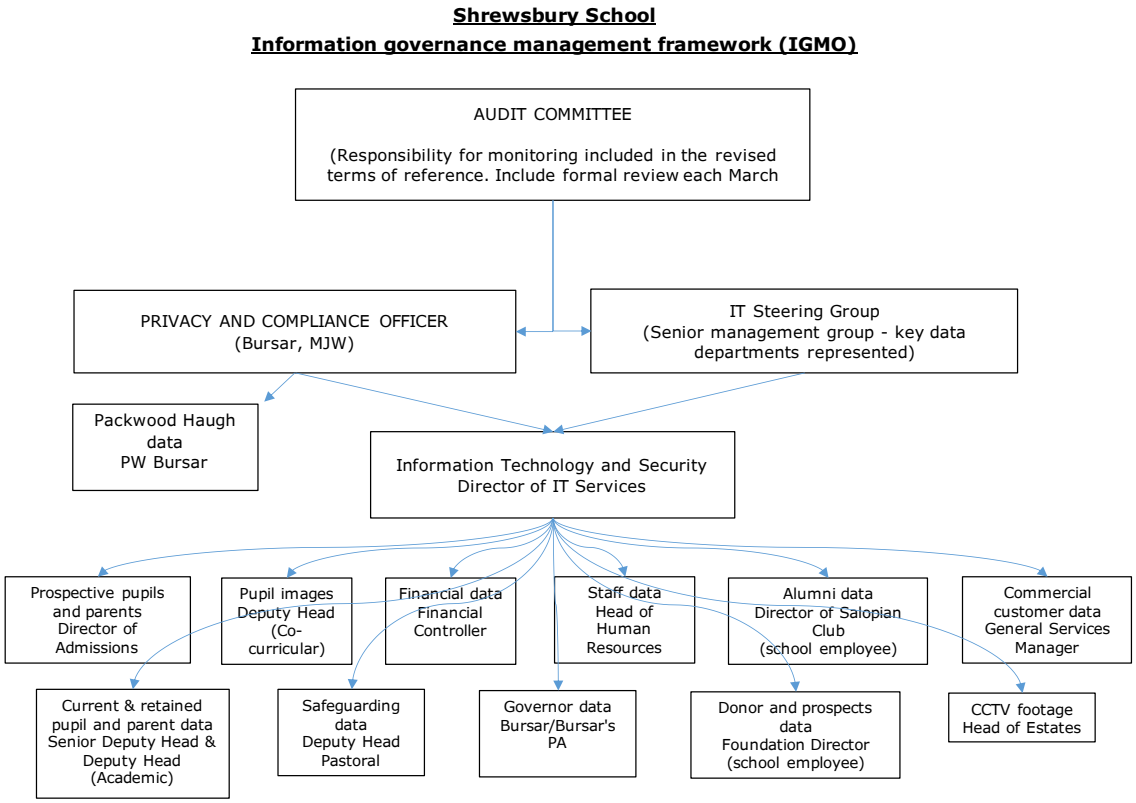
Owner: M Ware – Bursar

Reviewed September 2023

Next review September 2024

Appendix A

Organisation of data responsibilities within Shrewsbury School



Appendix B

SHREWSBURY SCHOOL

Privacy Notice

WHO WE ARE

For the purposes of Data protection legislation, the 'Data Controller' is Shrewsbury School, SY3 7BA. Our data protection registration number is **Z5306330**

This Privacy Notice is applicable to all the activities of the following organisations and associated bodies:

- Shrewsbury School, The Schools, Shrewsbury, SY3 7BA.
  Registered Charity Number 528413.
- Packwood Haugh School, Ruyton XI Towns, Shrewsbury, SY4 1HX (part of Registered Charity Number 528413)
- The Salopian Club, The Schools, The Schools, Shrewsbury, SY3 7BA.
- The Old Packwoodian Society, Ruyton XI Towns, Shrewsbury, SY4 1HX

The following organisations have separate privacy notices

- Shrewsbury School Foundation, The Schools, SY3 7BA. [**ZA511032]**
  Registered Charity Number 528415
- Shrewsbury School Trading Company Limited, The Schools, Shrewsbury, SY3 7BA. Company registration 05580019. **[ZA511020]**
- Shrewsbury School Enterprises Limited, The Schools, Shrewsbury, SY3 7BA. Company registration 04535585. **[ZA511016]**

WHAT THIS POLICY IS FOR

This policy is intended to provide information about how the School will process personal data about individuals including: its staff; its current, past and prospective pupils; and their parents, carers or guardians (referred to in this policy as "parents").

This information is provided in accordance with the rights of individuals under Data Protection Law to understand how their data is used. Staff, parents and pupils are all encouraged to read this Privacy Notice and understand the School's obligations to its entire community.

This **Privacy Notice** applies alongside any other information the School may provide about a particular use of personal data, for example when collecting data via an online or paper form.

This **Privacy Notice** also applies in addition to the School's other relevant terms and conditions and policies, including:

- any contract between the school and its staff or the parents of pupils;
- the School's data policies, including policies on taking, storing and using images of children;
- the School's policy on CCTV (Data Retention policy);
- the School's Data Security policy;
- the School's Child Protection and Safeguarding and health and safety policies, including how concerns or incidents are recorded; and

- the School's IT policies, including its pupil and non-pupil Acceptable Use policies, Cyber Bullying policy, Social Media Policy and Device for Learning policy.

Anyone who works for, or acts on behalf of, the School (including staff, volunteers, governors and service providers) should be aware of and comply with this Privacy Notice, which also provides further information about how personal data about those individuals will be used.

RESPONSIBILITY FOR DATA PROTECTION

- The School and associated bodies have appointed the Bursar as **Privacy and Compliance Officer** who will deal with all your requests and enquiries concerning the school's uses of your personal data (see section on *Your Rights* below) and endeavour to ensure that all personal data is processed in compliance with this policy and data protection law.

  The Bursar
  Shrewsbury School
  The Schools
  SY3 7BA

  01743 280820
  bursar@shrewsbury.org.uk

  Initial enquires related to Packwood Haugh data should be addressed to Natalie Shaw, Bursar, Packwood Haugh School ns@packwood-haugh.co.uk

WHY THE SCHOOL NEEDS TO PROCESS PERSONAL DATA

To carry out its ordinary duties to staff, pupils and parents, the School may process a wide range of personal data about individuals (including current, past and prospective staff, pupils or parents) as part of its daily operation.

Some of this activity the School will need to carry out in order to fulfil its legal rights, duties or obligations – including those under a contract with its staff, or parents of its pupils.

Other uses of personal data will be made in accordance with the School's legitimate interests, or the legitimate interests of another, if these are not outweighed by the impact on individuals and provided it does not involve special or sensitive types of data.

The School expects that the following uses may fall within that category of its (or its community's) "**legitimate interests**":

- For the purposes of pupil selection (and to confirm the identity of prospective pupils and their parents);
- To provide education services, including musical education, physical training (including swimming lessons) or spiritual development, career services, and extra-curricular activities to pupils, and monitoring pupils' progress and educational needs;
- Provision of commercial services such as hosting holiday camps, provision of swimming lessons, the promotion of performing arts events, and the organisation of sporting competitions on the school site;

- Maintaining relationships with alumni and the school community, including direct marketing or, except in the case of the Salopian Club, fundraising activity;
- For the purposes of donor due diligence, and to confirm the identity of prospective donors and their background and relevant interests;
- Collect information from publicly available sources about parents' and former pupils' occupation and activities in order to:
    - ensure our communications are relevant to you and your interests
    - to facilitate inclusion in all activities and events that our research helps us understand you may be interested in and
    - to maximise the School's philanthropic goals;
- For the purposes of management planning and forecasting, research and statistical analysis, including that imposed or provided for by law (such as diversity or gender pay gap analysis and taxation records);
- To enable relevant authorities to monitor the School's performance and to intervene or assist with incidents as appropriate;
- To give and receive information and references about past, current and prospective pupils, including relating to outstanding fees or payment history, to/from any educational institution that the pupil attended or where it is proposed they attend; and to provide references to potential employers of past pupils;
- To enable pupils to take part in national or other assessments, and to publish the results of public examinations or other achievements of pupils of the School;
- To safeguard pupils' welfare and provide appropriate pastoral care;
- To monitor (as appropriate) use of the School's IT and communications systems in accordance with the School's IT Acceptable Use Policy;
- To make use of photographic images of pupils in school publications, on the school website and (where appropriate) on the School's social media channels in accordance with the School's policy on taking, storing and using images of children;
- For security purposes, including CCTV in accordance with the School's CCTV policy;
- Organise transport to/from school at start and end of terms, Exeats and coach weekends; and
- Where otherwise reasonably necessary for the School's purposes, including to obtain appropriate professional advice and insurance for the School;
- Where appropriate, names and contact details of visitors to the school site, including pupils visiting from other schools for competitions or feeder school events.

In addition, the School may need to process **special category personal data** (concerning health, ethnicity, religion, biometrics or sexual life) or criminal records information (such as when carrying out DBS checks) in accordance with rights or duties imposed on it by law, including as regards safeguarding and employment, or from time to time by explicit consent where required. These reasons may include:

- To safeguard pupils' welfare and provide appropriate pastoral (and where necessary, medical) care, and to take appropriate action in the event of an emergency, incident or accident, including by disclosing details of an individual's medical condition where it is in the individual's interests to do so: for example, for medical advice, social services, insurance purposes or to organisers of school trips;
- To provide educational services in the context of any special educational needs of a pupil;
- To provide spiritual education in the context of any religious beliefs;

- In connection with employment of its staff, for example DBS checks, welfare or pension plans;
- To run any of its systems that operate on biometric data, such as for security and other forms of pupil or staff identification; or
- For legal and regulatory purposes (for example child protection, diversity monitoring and health and safety) and to comply with its legal obligations and duties of care;
- DBS information for trustees or volunteers.

TYPES OF PERSONAL DATA PROCESSED BY THE SCHOOL

This will include by way of example:

- names, addresses, telephone numbers, e-mail addresses and other contact details;
- car details (about those who use our car parking facilities);
- bank details and other financial information, eg about parents who pay fees to the School and about staff for payroll purposes;
- past, present and prospective pupils' academic, disciplinary, admissions and attendance records (including information about any special needs), and examination scripts and marks;
- where appropriate, information about individuals' health, and contact details for their next of kin;
- references given or received by the school about pupils, and information provided by previous educational establishments and/or other professionals or organisations working with pupils; and
- images of pupils (and occasionally other individuals) engaging in school activities, and images captured by the School's CCTV system (in accordance with the school's policy on taking, storing and using images of children & the CCTV policy).

HOW THE SCHOOL COLLECTS DATA

The School receives personal data from the individual directly (including, in the case of pupils, from their parents). This will be via a series of forms, in the ordinary course of interaction and communications such as letters, emails or written assessments.

Personal data may also be supplied by third parties (for example another school, or other professionals or authorities working with that individual), collected from publicly available resources or from previous schools/employers in the case of staff.

WHO HAS ACCESS TO PERSONAL DATA AND WHO THE SCHOOL SHARES IT WITH

Occasionally, the School will need to share personal information relating to its community with third parties, such as professional advisers (lawyers and accountants) or relevant authorities (HMRC, police or the local authority). The School may also share limited pupil details, such as name, email address, year group etc with selected third parties for the purposes of providing access to academic resources, extra-curricular activities eg MOD (CCF) and Duke of Edinburgh, external tutors and coaches and limited contact information with transport companies or taxi firms where arranging transport on a parent or pupils' behalf.

Details of food allergies or other relevant information may be shared with third party caterers and other schools where necessary to ensure safe delivery of catering or other services.

For the most part, personal data collected by the School will remain within the School and will be processed by appropriate individuals only in accordance with access protocols (ie on a 'need to know' basis). Particularly strict rules of access apply in the context of:

- medical records held and accessed only by the school doctor and appropriate medical staff under his/her supervision, or otherwise in accordance with express consent; and
- pastoral or safeguarding files.

Medical information may also be supplied to the School doctor's NHS practice via the NHS secure link.

A certain amount of any SEN pupil's relevant information will also need to be provided to staff more widely in the context of providing the necessary care and education that the pupil requires.

Staff, pupils and parents are reminded that the School is under duties imposed by law and statutory guidance (including **Keeping Children Safe in Education**) to record or report incidents and concerns that arise or are reported to it, in some cases regardless of whether they are proven, if they meet a certain threshold of seriousness in their nature or regularity. This may include file notes on personnel or safeguarding files, and in some cases referrals to relevant authorities such as the LADO or police. For further information about this, please view the School's Safeguarding Policy.

Finally, in accordance with data protection law, some of the School's processing activity is carried out on its behalf by third parties, such as IT systems, web developers or cloud storage providers. This is always subject to contractual assurances that personal data will be kept securely and only in accordance with the School's specific directions.

HOW LONG WE KEEP PERSONAL DATA

The School will retain personal data securely and only in line with how long it is necessary to keep for a legitimate and lawful reason. Typically, the legal recommendation for how long to keep ordinary pupil files is up to 7 years following departure from the School (or until age 25, whichever is the later, in the case of pupils). However, incident reports and safeguarding files will need to be kept much longer, in accordance with specific legal requirements. The Independent Enquiry into Child Sexual Abuse (IICSA) gives guidance on this matter and any data relating to actual or suspected child sexual abuse must be retained indefinitely. If you have any specific queries about how this policy is applied, or wish to request that personal data that you no longer believe to be relevant is considered for erasure, please contact The Bursar, **bursar@shrewsbury.org.uk** . However, please bear in mind that the School may have lawful and necessary reasons to hold on to some data.

The School's policy on Data Retention is contained within Appendix C of the Data Policies document.

KEEPING IN TOUCH AND SUPPORTING THE SCHOOL

The School and organisations listed above will use the contact details of parents, alumni and other members of the school community to keep them updated about the activities of the School, or alumni and parent events of interest, including by sending updates and newsletters, by email and by post. Unless the relevant individual objects, the School may also:

- Share personal data about parents and/or alumni, as appropriate, with organisations set up to help establish and maintain relationships with the school community, such as the Shrewsbury School Foundation, The Salopian Club, Shrewsbury School Parents' Association (SSPA);
- Contact parents and/or alumni (including via the Foundation, Salopian Club, SSPA or where applicable for Packwood Haugh School via the Old Packwoodian Society) by post and email to promote and raise funds for the School;
- Collect information from publicly available sources about parents' and former pupils' occupation and activities, in order to maximise the School's fundraising potential;

Should you wish to limit or object to any such use, or would like further information about them, please contact the Bursar in writing. You always have the right to withdraw consent, where given, or otherwise opt out of direct marketing or fundraising. However, the School may need nonetheless to retain some of your details (not least to ensure that no more communications are sent to that particular address, email or telephone number).

YOUR RIGHTS

Individuals have various rights under data protection law to access and understand personal data about them held by the School, and in some cases ask for it to be erased or amended or for the School to stop processing it, but subject to certain exemptions and limitations.

Any individual wishing to access or amend their personal data, or wishing it to be transferred to another person or organisation, or who has some other objection to how their personal data is used, should put their request in writing to the Bursar.

The School will endeavour to respond to any such written requests as soon as is reasonably practicable and in any event within statutory time-limits, which is one month in the case of requests for access to information. The School will be better able to respond quickly to smaller, targeted requests for information. If the request is manifestly excessive or similar to previous requests, the School may ask you to reconsider or charge a proportionate fee, but only where data protection law allows it.

You should be aware that certain data is exempt from the right of access. This may include information which identifies other individuals, or information which is subject to legal professional privilege. The School is also not required to disclose any pupil examination scripts (though examiners' comments may fall to be disclosed), nor any confidential reference given by the School for the purposes of the education, training or employment of any individual.

PUPIL REQUESTS

Pupils can make subject access requests for their own personal data, provided that, in the reasonable opinion of the School, they have sufficient maturity to understand the request they are making (see section *Whose Rights* below). Indeed, while a person with parental responsibility will generally be entitled to make a subject access request on behalf of younger pupils, the information in question is always considered to be the child's at law.

A pupil of any age may ask a parent or other representative to make a subject access request on his/her behalf. Moreover (if of sufficient age) their consent or authority may need to be sought by the parent making such a request. Pupils *aged 13 and above* are generally assumed to have this level of maturity, although this will depend on both the child and the personal data requested, including any relevant circumstances at home.

All information requests from, or on behalf of, pupils – whether made under subject access or simply as an incidental request – will therefore be considered on a case by case basis.

CONSENT

Where the School is relying on consent as a means to process personal data, any person may withdraw this consent at any time (subject to similar age considerations as above). Please be aware however that the School may have another lawful reason to process the personal data in question even without your consent.

That reason will usually have been asserted under this Privacy Notice or may otherwise exist under some form of contract or agreement with the individual (eg an employment or parent contract, or because a purchase of goods, services or membership of an organisation such as an alumni or parents' association has been requested).

WHOSE RIGHTS

The rights under data protection law belong to the individual to whom the data relates. However, the School will often rely on parental consent to process personal data relating to pupils (if consent is required) unless, given the nature of the processing in question, and the pupil's age and understanding, it is more appropriate to rely on the pupil's consent.

Parents should be aware that in such situations they may not be consulted, depending on the interests of the child, the parents' rights at law or under their contract, and all the circumstances.

In general, the School will assume that pupils' consent is not required for ordinary disclosure of their personal data to their parents, eg for the purposes of keeping parents informed about the pupil's activities, progress and behaviour, and in the interests of the pupil's welfare, unless, in the School's opinion, there is a good reason to do otherwise.

However, where a pupil seeks to raise concerns confidentially with a member of staff and expressly withholds their agreement to their personal data being disclosed to their parents, the School may be under an obligation to maintain confidentiality unless, in the School's opinion, there is a good reason to do otherwise; for example where the School believes disclosure will be in the best interests of the pupil or other pupils, or if required by law.

Pupils are required to respect the personal data and privacy of others, and to comply with the School's Pupil Acceptable Usage Policy and the school rules. Staff are under professional duties to do the same covered under the relevant Non-pupil Acceptable Usage and staff policies.

DATA ACCURACY AND SECURITY

The School will endeavour to ensure that all personal data held in relation to an individual is as up to date and accurate as possible. Individuals must please notify the Bursar of any significant changes to important information, such as contact details, held about them.

An individual has the right to request that any out-of-date, irrelevant or inaccurate or information about them is erased or corrected (subject to certain exemptions and limitations under data protection law): please see above for details of why the School may need to process your data, of who you may contact if you disagree.

The School will take appropriate technical and organisational steps to ensure the security of personal data about individuals, including policies around use of technology and devices,

and access to school systems. All staff and governors will be made aware of this policy and their duties under data protection law and receive relevant training.

THIS POLICY

The School will update this Privacy Notice from time to time. Any substantial changes that affect your rights will be provided to you directly as far as is reasonably practicable.

QUERIES AND COMPLAINTS

Any comments or queries on this policy should be directed to the Bursar using the following contact details.

The Bursar
Shrewsbury School
The Schools
SY3 7BA

01743 280820
bursar@shrewsbury.org.uk

If an individual believes that the School has not complied with this policy or acted otherwise than in accordance with data protection law, they should utilise the school complaints procedure and should also notify the Bursar. The individual can also make a referral to or lodge a complaint with the Information Commissioner's Office (ICO), although the ICO recommends that steps are taken to resolve the matter with the school before involving the regulator.

Owner: M Ware - Bursar

Reviewed September 2023

Next review September 2024

Appendix C

SHREWSBURY SCHOOL

Data storage and retention guidelines

The **data holder** for each area of school data is responsible for the safe custody of that data, and for ensuring that the data is not retained for longer than is justified by the relevance and purpose of that data.

Particular considerations in respect of data retention:

- Statutory requirements
- Contractual requirements
- Relevance and purpose of the data held
- Balance between the legitimate purposes of the organisation in holding the personal data and the rights and freedoms of the individual data subject
- Balancing the burden of security responsibilities for the data vs the organisational requirement

Data erasure and destruction

Data erasure or destruction should be approved by the Director of IT for digital records, or by an approved secure disposal contractor for paper records. The Privacy and Compliance Officer will be able to supply details of "secure disposal" contractors approved by the school.

Table of guideline retention periods

The table below provides guidance for data holders but there may be occasions when the data holder needs to take into account the particular considerations of an individual case.

Data Holder	Type of record/document	Retention period
HM Office (DH Academic)	Pupil academic records	Until subject aged 25
HM Office (DH Pastoral)	Pupil pastoral records	Until subject aged 25
DH Academic	SEN records	Until subject aged 35
Bursar	Parent administrative records	7 years after child leaves school
Director of Admissions	Pupil admissions records	7 years after pupil leaves
Director of Admissions	Application records (those who do not come to the school)	5 years after applications for prospective pupils who do not come to the school
Designated Safeguarding Lead	Safeguarding records	Permanent
Bursar	Accident records	Life span of individual affected
Financial Controller	Accounting records	6 years
Head of Human Resources	Single Central Record (not DBS certificate itself)	6 years

Financial controller	Pay roll data	6 years
Clerk to Governors	Trustee personal data	10 years after completion of term (some archive material retained)
Head of Human Resources	Unsuccessful job applicants	6 months after application
Head of Human Resources	Pension or benefits information	Lifespan of employee
Head of Human Resources	Staff personnel data	Indefinitely: At least Lifespan of employee (note obligations for safeguarding in the sector)
General Services Manager	Commercial customer data (limited personal data)	3 years
Director of Salopian Club	Club member records	Lifespan of club member (unless objection received)
Director of Foundation	Alumni and Friend records	Lifespan of data subject (unless objection received)
D/H Co-curricular	Pupil images	Retention period will vary (some archive footage will be permanent)
Packwood Haugh Bursar	Packwood Haugh Data	Retention periods apply as above with the exception of - Academic records for PW pupils for 7 years after they leave - Admissions and application records for PW pupils until pupil is 25

Appendix D

SHREWSBURY SCHOOL

Data breach management procedures

Through the following measures the school hopes to reduce the risk of a "data breach":

- Clear data and IT policies
- appropriate staff training
- careful management of third party data processors
- appropriate risk management of data processes (privacy impact assessments)

However, the risk cannot be completely eliminated and this appendix details the School's processes to identify and react to data breaches.

What is a data breach?

If personal data which the School holds in respect of pupils, staff, governors, alumni etc is lost or distributed outside of the organisation without the necessary permissions or controls, this is described as a ***data breach***. It could also mean "unauthorised access" to data as well as loss of data. A data breach could relate to electronic or paper records. It could occur where a school device is lost and does not have appropriate password, encryption or other security controls over the personal data held on it.

The volume and sensitivity of the personal data lost will dictate the School's response and reporting obligations, but we will log all data breaches in order to identify risks and improve controls over data. The school has a duty to report data breaches to the **Information Commissioner's Office (ICO)** where there is a risk posed to data subjects' rights and freedoms. Such reports have to be made within 72 hours of the School becoming aware of the breach.

What to do when a data breach is discovered

1) Inform the Bursar

   If you become aware of a data breach, inform the Bursar who is Privacy and Compliance Officer and will be responsible for managing the response and reporting of a data breach, also cc ITsupport@shrewsbury.org.uk

2) Logging incident and assessing next steps

   The Privacy and Compliance Officer will log the data breach, and assess containment actions, reporting obligations and prevention actions.

   The Privacy and Compliance Officer will consider the following:

   - The volume of data affected by the breach
   - The sensitivity of personal data
   - Risk to individual rights (risk of fraud, personal embarrassment or loss of privacy)

   At this stage the Privacy and Compliance Officer will consider whether the data breach needs to be escalated to the Critical Incident Management Committee.

3) Initial reaction (containment and recovery)

- How long has the breach been active, what data was involved and how far has it got?
- What immediate steps can be taken to prevent it going further? Consider:
    - if a cyber breach, involve the School's Director of IT from the outset;
    - if human factor(s) are involved, can the individuals be contacted to give reassurances;
    - if eg Royal Mail, courier, IT or other contractors are involved, can they assist;
    - are specialists needed: forensic IT consultants, crisis management PR, legal etc
- Build up a more detailed picture of the risk and reach of the security breach:
    - how many have been affected?
    - was any sensitive personal data involved – health, sexual life, crime?
    - was financial data involved and/or is there a risk of identify fraud?
- Identify if a crime has been committed and involve police or cyber fraud unit.
- Assess if insurers need notifying (major loss, crime, or possible legal claim(s))
- Decide if the likely risk of harm to the data subjects:
    - is sufficient to require a full or preliminary notification to the ICO; and
    - is sufficiently serious to require communication to affected individuals
- If not, is this a matter we can document but deal with internally? or
- If so, what can we usefully tell the ICO and/or individuals at this stage?
    - eg provide fraud or password advice, offer counselling etc.

4) On-going reaction (containment and recovery)

a) Continue to monitor and assess possible consequences (even if apparently contained).
b) Keep the ICO and/or those affected informed as new information becomes available.
c) Tell the ICO and/or those affected what you are doing to remediate and improve practice.
d) Begin process of review internally:
    a. how did this happen? What could we have done better?
    b. would training or even disciplinary action be justified for staff members?
    c. were our policies adequate, and/or adequately followed?
    d. if our contractors were involved (eg systems providers), did they respond adequately? Do we have any remedies against them if not?

5) Record keeping and putting outcomes into practice

   a) Keep a full internal record, whether or not the matter was reported or resulted in harm.
   b) Log this record against wider trends and compare with past incidents.
   c) Make sure all past outcomes were in fact put into practice.
   d) Ensure any recommendations made by, or promised to, the ICO are actioned.
   e) Notify ***the Charity Commission as an RSI (report of serious incident),*** at an appropriate juncture.
   f) Review policies and ensure regular (or specific, if required) training is actually completed.

Reporting and contact details

Serious breaches should be reported to the ICO using the security breach helpline on 0303 123 1113 (open Monday to Friday, 9am to 5pm). Select option 3 to speak to staff who will record the breach and give advice.

Or, use the security breach notification form, which should be sent to the email address: casework@ico.org.uk

or by post to the ICO office address: Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF.

The security breach notification form can be found here:

https://ico.org.uk/media/fororganisations/documents/2666/security_breach_notification_form.doc

Appendix D

SHREWSBURY SCHOOL
TAKING, STORING AND USING IMAGES POLICY

1. INTRODUCTION

1.1 This policy is intended to provide information to pupils and their parents, carers or guardians (referred to in this policy as 'parents') about how images and videos of pupils are normally used by Shrewsbury School ('the School'). It applies in addition to the School's Terms & Conditions and more general information about use of pupils' personal data such as the School's Privacy Notice.

2. RELATED POLICIES

2.1 This policy should be read in conjunction with the following School policies:

- Staff Code of Conduct
- Non Pupil IT Acceptable Use Policy
- Child Protection and Safeguarding Policy
- The School's Privacy Notice
- Social Media Policy
- Data Protection Policy
- Drones Policy

3. GENERAL POINTS

3.1 Certain uses of images and videos are necessary for the ordinary running of the School; other uses are in the legitimate interests of the School and its community and unlikely to cause any negative impact on children. The School is entitled lawfully to process such images and take decisions about how to use them, subject to any reasonable objections raised.

3.2 Parents who accept a place for their child at the School are invited to agree to the School using images of their child as set out in this policy via the School's Terms & Conditions.

3.3 It is hoped that parents will feel able to support the School in using pupils images and videos to celebrate the achievements of pupils (whether sporting, academic or otherwise) to promote the work of the School and for important administrative purposes such as identification and security.

3.4 Any parent who wishes to limit the use of images or videos of a pupil for whom they are responsible should contact in writing the Bursar in their capacity as Data Controller. The School will respect the wishes of parents (and indeed pupils

themselves) wherever reasonably possible, and in accordance with this policy and the Data Protection Act 2018 and General Data Protection Regulation (GDPR).

3.5 Parents should be aware that from the age of 13 upwards, the law recognises pupils' own rights to have a say in how their personal information is used – including images.

4. USE OF PUPIL IMAGES IN SCHOOL PUBLICATIONS

4.1 The School routinely uses images and videos of its pupils to keep the School community updated on the activities of the School and for marketing and promotional purposes, including:

i. On internal displays on digital and conventional notice boards within the School premises;

ii. In communications with the School community (parents, pupils, staff, Governors and alumni) including by e-mail, on the School intranet and by post;

iii. On the School's website and via the School's social media and digital channels (such as Twitter, Instagram, LinkedIn, YouTube, Vimeo and Facebook).

iv. In the School's literature, website(s), press and other external advertisements for the School. Such external advertising would not normally include pupil's names (and the School may seek the parent and/or pupil's specific consent, depending on the nature of the image or the use).

5. USE OF PUPIL IMAGES FOR IDENTIFICATION AND SECURITY

5.1 For the purposes of internal identification, all pupils are photographed on entering the School and, thereafter, again as they enter the Sixth Form. These photographs identify the pupil by name, year group and House.

5.2 CCTV is in use on School premises, and will sometimes capture images of pupils. Images captured on the School's CCTV system are used in accordance with the Privacy Notice and CCTV policy.

6. USE OF PUPILS IMAGES AND VIDEO IN THE MEDIA

6.1 Where practicably possible, the School will notify parents in advance when the media is expected to attend an event or School activity in which School pupils are participating, and will make every reasonable effort to ensure that any pupil whose parent has refused permission for images of that pupil, or themselves, to be used in these circumstances are not photographed or filmed by the media, nor such images provided for media purposes.

6.2 In such circumstances where the media requests the names of pupils to accompany images, these will be provided where parents have been informed about the media's visit and both parent and pupil has consented as appropriate.

6.3 General Data Protection Regulation allows all customers to revoke permissions from the use of personal data and imagery and all subsequent content must be removed in an appropriate timeline depending on the use of the data/imagery.

6.4 Any School social media channels including any protected and/or locked Shrewsbury School accounts on social media, such as House accounts, must not feature any content or imagery illustrating alcohol consumption or any other activity deemed to be inappropriate for those aged under the relevant legal age. Further guidance on use of photographs and videos involving pupils can also be found in Appendix 5 of the Staff Code of Conduct.

7. SECURITY OF PUPIL IMAGES

7.1 Professional photographers and the media are accompanied at all times by a member of staff when on School premises. The School only uses reputable professional photographers and makes every effort to ensure that any images of pupils are held by them securely, responsibly and in accordance with the School's instructions.

7.2 The School takes appropriate technical and organisational security measures to ensure that images and videos of pupils held by the School are kept securely on School systems, and protected from loss or misuse. The School will take reasonable steps to ensure that members of staff only have access to images of pupils held by the School where it is necessary for them to do so this is reflected in the Mobile Telephone Policy and the IT Acceptable Use Policy.

8. USE OF CAMERAS AND FILMING EQUIPMENT (INCLUDING MOBILE PHONES) BY PARENTS

8.1 Staff are permitted to take photographs and videos on school-owned devices for school purposes only and must be stored or deleted as per GDPR guidelines.

8.2 Parents and carers are permitted to take photographs and footage for their personal use only. If they choose to share these images in the public domain (i.e. social media), they should be mindful of including others who may not have given their consent. The opportunity of parents/carers to take images can be restricted by the

School where it is not appropriate and the School reserves the right to withdraw consent at any time.

8.3 The School may record or stream events, plays and concerts professionally (or commission a professional photographer or film company to do so) in which case DVD or digital copies may be made available to parents for purchase. Parents of pupils taking part in such plays and concerts will be consulted if it is intended to make such recordings available more widely.

9. USE OF CAMERAS AND FILMING EQUIPMENT (INCLUDING MOBILE PHONES) BY PUPILS

9.1 All pupils are encouraged to look after each other, and to report any concerns about the misuse of technology, or any worrying issues to the Senior Deputy Head and/or the Deputy Head Pastoral.

9.2 The use of cameras or filming equipment (including on mobile phones) is not allowed in toilets, washing or changing areas, nor should photography or filming equipment be used by pupils in a manner that may offend or cause upset.

9.3 The misuse of images, cameras or filming equipment in a way that breaches this Policy, or the School's Anti-Bullying Policy, IT Acceptable Use Policy for Pupils, Safeguarding Policy or the School's Rules is always taken seriously, and may be the subject of disciplinary procedures or dealt with under the relevant safeguarding policy as appropriate.

Owner: G Ferriday – Director of Marketing and Communications

Reviewed September 2023

Next review September 2024

Appendix F

SHREWSBURY SCHOOL

CCTV POLICY

The purpose of this policy is to regulate the management and operation of the Closed Circuit Television (CCTV) System at Shrewsbury School (the **School**). It also serves as a notice and a guide to data subjects (including pupils, parents, staff, volunteers, visitors to the School and members of the public) regarding their rights in relation to personal data recorded via the CCTV system (the **System**).

The System is administered and managed by the School, who acts as the Data Controller. This policy will be subject to review from time to time, and should be read with reference to the School's Privacy Notice (Appendix B of the Data Policies document).

All fixed cameras are in plain sight on the school premises and the School does not routinely use CCTV for covert monitoring or monitoring of private property outside the School grounds. (The Head of Estates maintains a list of camera locations.)

The School's purposes of using the CCTV system are set out below and, having fully considered the privacy rights of individuals, the School believes these purposes are all in its legitimate interests. Data captured for the purposes below will not be used for any commercial purpose.

1. Objectives of the System

1.1 To protect pupils, staff, volunteers, visitors and members of the public with regard to their personal safety (including management of vehicles).

1.2 To protect the School buildings and equipment, and the personal property of pupils, staff, volunteers, visitors and members of the public.

1.3 To support the police and community in preventing and detecting crime, and assist in the identification and apprehension of offenders.

1.4 To monitor the security and integrity of the School site and deliveries and arrivals.

1.5 To monitor staff and contractors when carrying out work duties.

1.6 To monitor and uphold discipline among pupils in line with the School Rules, which are available to parents and pupils on request.

2. Positioning

2.1 Locations have been selected, both inside and out, that the School reasonably believes require monitoring to address the stated objectives.

2.2 Adequate signage has been placed in prominent positions to inform staff and pupils that they are entering a monitored area, identifying the School as the Data Controller and giving contact details for further information regarding the system.

2.3 No images will be captured from areas in which individuals would have a heightened expectation of privacy, including changing and washroom facilities.

2.4 No images of public spaces will be captured except to a limited extent at site entrances.

3. Maintenance

3.1 The CCTV system will be operational 24 hours a day, every day of the year.

3.2 The System Manager (defined below) will check and confirm that the system is properly recording and that cameras are functioning correctly, on a regular basis.

3.3 The system will be checked and (to the extent necessary) serviced no less than annually.

4. Supervision of the System

4.1 Staff authorised by the School to conduct routine supervision of the system may include School Shop staff, site wardens, supervisors at the sports centre and relevant staff on duty.

4.2 Images will be viewed and/or monitored in a suitably secure and private area to minimise the likelihood of or opportunity for access to unauthorised persons.

5. Storage of Data

5.1 The day-to-day management of images will be the responsibility of the Head of Estates who will act as the System Manager, or such suitable person as the System Manager shall appoint in his or her absence.

5.2 Images will be stored for (eg 2-4 weeks), and automatically over-written unless the School considers it reasonably necessary for the pursuit of the objectives outlined above, or if lawfully required by an appropriate third party such as the police or local authority.

5.3 Where such data is retained, it will be retained in accordance with the Act and our ***Privacy Notice*** and ***Data storage and retention procedures***. Information including the date, time and length of the recording, as well as the locations covered and groups or individuals recorded, will be recorded in the system log book.

6. Access to Images

6.1 Access to stored CCTV images will only be given to authorised persons, under the supervision of the System Manager, in pursuance of the above objectives (or if there is some other overriding and lawful reason to grant such access).

6.2 Individuals also have the right to access personal data the School holds on them (please see the Privacy Notice), including information held on the system, if it has been kept. The School will require specific details including at least to time, date and camera location before it can properly respond to any such requests. This right is subject to certain exemptions from access, including in some circumstances where others are identifiable.

6.3 The System Manager must satisfy themselves of the identity of any person wishing to view stored images or access the system and the legitimacy of the request. The following are examples when the System Manager may authorise access to CCTV images:

6.3.1 Where required to do so by the Head, the Bursar, the Police or some relevant statutory authority;

6.3.2 To make a report regarding suspected criminal behaviour;

6.3.3 To enable the Designated Safeguarding Lead or his/her appointed deputy to examine behaviour which may give rise to any reasonable safeguarding concern;

6.3.4 To assist the School in establishing facts in cases of unacceptable pupil behaviour, in which case, the parents/guardian will be informed as part of the School's management of a particular incident;

6.3.5 To data subjects (or their legal representatives) pursuant to an access request under the Act and on the basis set out in 6.2 above;

6.3.6 To the School's insurance company where required in order to pursue a claim for damage done to insured property; or

6.3.7 In any other circumstances required under law or regulation.

6.4 Where images are disclosed under 6.3 above a record will be made in the system log book including the person viewing the images, the time of access, the reason for viewing the images, the details of images viewed and a crime incident number (if applicable).

7. Complaints and queries

7.1 Any complaints or queries in relation to the School's CCTV system, or its use of CCTV, or requests for copies, should be referred to the Bursar.

Owner: J Taylor – Head of Estates

Reviewed September 2023

Next review September 2024

CCTV FOOTAGE ACCESS REQUEST

The following information is required before the school can provide copies of or access to CCTV footage from which a person believes they may be identified.

Please note that CCTV footage may contain the information of others that needs to be protected, and that the school typically deletes CCTV recordings after a 30-day period.

Name and address: (proof of ID may be required)	
Description of footage (including a description of yourself, clothing, activity etc.)	
Location of camera	
Date of footage sought	
Approximate time (give a range if necessary)	

Signature*……

Print Name…….

Date ……..

*** NB For children 13 or over, the child's authority or consent must be obtained except in circumstances where that would clearly be inappropriate and the lawful reasons to provide to the parent(s) outweigh the privacy considerations of the child.**