Policy / Procedure Cover Sheet

Policy/Procedure	Data Protection Policy		
Type	Operational		
Applies to project(s)	Watermelon Independent Schools	**Policy No**	OP/11
Created by(owner)	Z Jonah		
Status	Released		
Date	Jan 2026		
Next review date:	Jan 2027		

Change History:

Version	**Description**	**Date issued**	**Reason**	**Approved by**
1.0	New policy	18.07.2024	New School	ZJ
1.1	Review	July 2025	Review	HL
1.2	Review	Jan 2026	Review	HL

Related policies:

Policy Ref No.	Policy Name	Policy Ref No.	Policy Name
S/02	E Safety	S/01	Child protection and Safeguarding
OP/07	Complaints Policy and Procedure		Privacy Notices
OP/19	Information Security Policy	S/02	E Safety Policy

Distribution:
Electronic copy - Company Policies and Procedures/
Hard copies – All Employees, School Office / Staff Reference Folder

This Data Protection Policy should be read in conjunction with the following policies:

i. ICT and Acceptable Use Policy
ii. Information and Security Policy
iii. Safeguarding Policy
iv. Privacy Notices

GDPR Policy
Contents

Appendix

1 Aims

1.1 Watermelon Independent Schools aims to ensure that all personal data collected about staff, students, parents and carers, governors, visitors and other individuals is collected, stored and processed in accordance with the UK data protection law.

1.2 The School recognises data protection is more than just a legal compliance. We recognise that respecting the confidentiality of personal data is critical to preserving the trust of our staff, students, parents/carers, visitors and other individuals for building the foundations for a strong relationship with all in the school's community and beyond. Through developing systems for the protection and security of data, the School is making a commitment to treat all personal data with care and respect.

1.3 This policy and any other documents referred to in it set out the basis on which we will process any personal data we collect from data subjects, or that is provided to us by data subjects or other sources.

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

1.5 This policy applies to all personal data, regardless of whether it is in paper or electronic format.

Legislation and guidance

2.1 The Company takes its obligations under the Data Protection Act 2018 (DPA 2018) and the UK General Data Protection (UK GDPR) Regulation seriously. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests.

2.2 The policy reflects the ICO's code of practice / guidance on the UK GDPR and guidance from the Department of Education (DfE) on Generative artificial intelligence in education. It also reflects the ICO's guidance for the use of surveillance cameras and personal information. In addition, this policy complies with Regulation 5 of the Education (Pupil Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record.

3 Policy Statement

3.1 The School needs to collect and use certain types of personal information about people with whom it deals in order to operate. These include current, past and prospective employees, students, suppliers, clients, and others with whom it communicates. In addition, it may be required by law to collect and use certain types of information to comply with the requirements of government departments. This personal information must be dealt with properly however it is collected, recorded and used - whether on paper, in a computer, or recorded on other material.

3.2 We regard the lawful and correct treatment of personal information by the School as very important in order to secure the successful carrying out of operations and the delivery of our services, and to maintaining confidence with those whom we deal. The School wishes to ensure that it treats personal information lawfully, correctly and in compliance with GDPR.

3.3 The School will implement this policy in line with the principles of the Equality Act 2010 and with due regard to an employee's disability and the Company's duty to make reasonable adjustments to

Its arrangements, policies and procedures, where applicable.

4 Definitions

Term	Definition
Personal Data	Any information relating to an identified, or identifiable, individual. This may include the individual's: • Name (including initials) • Identification number • Location data • Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special Categories of Personal Data	Personal data which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health – physical or mental • Sex life or sexual orientation.
Processing	Anything done to personal data, such as collecting, recording, organizing, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data Subject	The identified or identifiable individual whose personal data is held or processed.
Data Controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data Processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal Data Breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

5 The data controller

5.1 Everyone has rights with regard to the way in which their personal data is handled. During the course of our activities as an educational setting, we will collect, store and process personal data about our staff, students, parents/carers, volunteers, visitors and others. This makes us a data controller in relation to that personal data.

5.2 Our school processes personal data personal data relating to parents and carers, pupils, staff,

governors, visitors and others, and therefore is a data controller.

5.3 Watermelon Independent Schools is registered as a data controller with the ICO as legally required and will renew this registration annually or as otherwise legally required. Registration No. ZA695571.

6 Roles and responsibilities

6.1 This policy applies to all staff employed by our school, and to external organizations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

6.2 Proprietor

The proprietor has overall responsibility for ensuring that the school complies with all relevant data protection obligations.

6.3 Data Protection Officer

The Data Protection Officer (DPO) is responsible for providing advice and guidance to the Watermelon Independent Schools in order to assist the School to implement this policy, monitor compliance with data protection law, and develop related policies and guidelines where applicable. The DPO will carry out an annual audit of the school's data processing activities and report to the Proprietor and Headteacher their advice and recommendations on the school's data protection issues. The DPO is also the first point of contact for individuals whose data the school processes, and for the ICO.

Our DPO is the School DPO Service and is contactable via Husein@watermelonschools.com or alternatively;

School Data Protection Officer, Watermelon Schools, Redfern Road, Birmingham, B11 2BE

6.4 Headteacher

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

6.5 Data Protection Lead

Watermelon Independent Schools has nominated the following individual as designated person to be contacted internally in relation to all matters relating to data protection issues, and to make referrals, where necessary, on referrals@watermelonschools.com. Should they be unavailable, issues should be referred to a member of the senior leadership team.

6.5 All staff

All members of staff must be aware of their duties and responsibilities towards the protection of personal data and adhering to this policy. Any breach of this policy may result in disciplinary or other action.

Staff are responsible for:

i. collecting, storing and processing any personal data in accordance with this policy
ii. informing the school of any changes to their personal data, such as a change of address
iii. contacting the school's designated Data Protection Lead in the following circumstances:

- with any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
- if they have any concerns that this policy is not being followed
- if they are unsure whether or not they have a lawful basis to use personal data in a p articular way
- if they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
- if there has been a data breach
- whenever they are engaging in a new activity that may affect the privacy rights of individuals
- if they need help with any contracts or sharing personal data with third parties.

7 Data Protection Principles –

7.1 The GDPR is based on data protection principles that the School must comply with. Watermelon Independent Schools has adopted the principles to underpin its Data Protection Policy:

7.2 The principles require that all personal data shall be:

i. processed lawfully, fairly and in a transparent manner ('lawfulness, fairness and transparency')
ii. used for specified, explicit and legitimate purposes ('purpose limitation')
iii. used in a way that is adequate, relevant and limited to what is necessary to fulfil the purpose for which it is processed ('data minimisation')
iv. accurate and, where necessary, kept up to date
v. kept no longer than is necessary for the purposes for which it is processed ('storage limitation')
vi. processed in a manner that ensures it is appropriately secure

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

7.4 For personal data to be processed fairly, data subjects must be made aware:

i. that the personal data is being processed
ii. why the personal data is being processed
iii. what the lawful basis is for that processing (see below)
iv. whether the personal data will be shared, and if so with whom
v. the period for which the personal data will be held
vi. the existence of the data subject's rights in relation to the processing of that personal data
vii. the right of the data subject to raise a complaint with the ICO in relation to any processing.

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

8 Collecting personal data

8.1 Lawfulness, fairness and transparency

8.1.1 Watermelon Independent Schools shall only process personal data where it has *one of six* 'lawful bases' (legal reasons)
available to the school to do so under data protection law:

i. the data needs to be processed so that the School can **fulfil a contract** with the individual, or the individual has asked the School to take specific steps before entering into a contract
ii. the data needs to be processed so that the School can **comply with a legal obligation**
iii. the data needs to be processed to ensure the **vital interests** of the individual or another person e.g. to protect someone's life
iv. the data needs to be processed so that the school, as a public authority, can perform a task in the **public interest**, or **exercise its official authority**
v. the data needs to be processed for the **legitimate interests** of the school (where the processing is not for any tasks the school performs as a public authority) or a third party, provided the individual's rights and freedoms are not overridden
vi. the individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear **consent**

8.1.2 For special categories of personal data, we will also meet one of the special category conditions for processing which are set out under data protection law:

i. The individual (or their parent/carer when appropriate in the case of a pupil) has given **explicit consent**
ii. The data needs to be processed to perform or exercise obligations or rights in relation to **employment, social security or social protection law**
iii. The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent
iv. The data has already been made **manifestly public** by the individual
v. The data needs to be processed for the establishment, exercise or defence of **legal claims**
vi. The data needs to be processed for reasons of **substantial public interest** as defined in legislation
vii. The data needs to be processed for **health or social care purposes**, and the processing is done by, or under the direction of, a health or social work professional or by any other person obliged to confidentiality under law
viii. The data needs to be processed for **public health reasons**, and the processing is done by, or under the direction of, a health professional or by any other person obliged to confidentiality under law
ix. The data needs to be processed for **archiving purposes**, scientific or historical research purposes, or statistical purposes, and the processing is in the public interest

8.1.3 For criminal offence data, we will meet both a lawful basis and a condition set out under data protection law. Conditions include:

i. The individual (or their parent/carer when appropriate in the case of a pupil) has given consent
ii. The data needs to be processed to ensure the vital interests of the individual or another person, where the individual is physically or legally incapable of giving consent
iii. The data has already been made manifestly public by the individual
iv. The data needs to be processed for or in connection with legal proceedings, to obtain legal advice, or for the establishment, exercise or defence of legal rights
v. The data needs to be processed for reasons of **substantial public interest** as defined in legislation

8.1.4 Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

8.1.5 We will always consider the fairness of our data processing. We will ensure we do not handle personal data in ways that individuals would not reasonably expect or use personal data in ways which have unjustified adverse effects on them.

8.1.6 If we offer online services to students, such as classroom apps, and we intend to rely on consent as a basis for processing, we will get parental consent where the student is under 13 (except for online counselling and preventive services). Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

8.2 Limitation, minimisation and accuracy

8.2.1 We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data. If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so and seek consent where necessary.

8.2.2 Staff must only process personal data where it is necessary in order to do their jobs. When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the school's record retention schedule.

9 Sharing personal data

9.1 We will not normally share personal data with anyone else without consent, but there are certain circumstances where we may be required to do so. These include, but are not limited to, situations where:

i. there is an issue with a student or parent/carer that puts the safety of our staff at risk
ii. we need to liaise with other agencies – we will seek consent as necessary before doing so
iii. our suppliers or contractors need data to enable us to provide services to our staff and students – for example, IT companies. When doing this, we will:

- only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
- establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share
- only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

9.2 We will also share personal data with law enforcement and government bodies where we are legally required to do so, including:

i. the prevention or detection of crime and/or fraud
ii. the apprehension or prosecution of offenders
iii. the assessment or collection of tax owed to Her Majesty's Revenue and Customs (HMRC)
iv. in connection with legal proceedings
v. where the disclosure is required to satisfy our safeguarding obligations
vi. research and statistical purposes, as long as personal data is sufficiently anonymised, or consent has been provided.

9.3 We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our students or staff.

9.4 Where we transfer personal data internationally, we will do so in accordance with UK data protection law

10 Subject access requests and other rights of individuals

10.1 Subject access requests

10.1.1 Individuals have a right to make a 'subject access request' to gain access to personal information that the School holds about them. This includes:

i. confirmation that their personal data is being processed
ii. access to a copy of the data
iii. the purposes of the data processing
iv. the categories of personal data concerned
v. who the data has been, or will be, shared with
vi. how long the data will be stored for, or if this isn't possible, the criteria used to determine this period
vii. the source of the data, if not the individual
viii. where relevant, the existence of the right to request rectification, erasure or restriction, or to object to such processing
ix. the right to lodge a compliant with the ICO or another supervisory authority
x. the source of the data, if not the individual
xi. whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual
xii. the safeguards provided if the data is being transferred internationally

10.1.2 Subject access requests can be made verbally or in writing. A request is valid if it is clear that the individual is asking for their own personal data. An individual may ask a third party to make a SAR on their behalf. Before responding, the DPO will need to be satisfied that the third party making the request is entitled to act on behalf of the individual.

10.1.3 To ensure that the request is responded to accurately, the applicant should be encouraged to make the request in writing and set out:

i. name of individual
ii. name of the school
iii. correspondence address
i. contact number and email address
ii. details of the information requested

10.1.4 The DPO will send the subject request to the Data Protection Lead. If staff receive a subject access request, they must immediately forward it to the Data Protection Lead, who will ensure that the DPO is informed. Information to be released, will be collated by the School and then sent to the DPO for checking and sending out to the applicant.

10.2 Children and subject access requests

10.2.1 Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the person should have parental responsibility for the child, and the child must either be unable to understand their rights and the implications of a subject access request or have given their consent.

10.2.2 Children aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from those with parental responsibility for pupils at our school may not be granted without the express permission of the student. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

10.2.3 Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from those with parental responsibility for pupils at our school [aged under 12] will in general be granted without requiring the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

10.3 Responding to subject access requests

10.3.1 When responding to requests, we:

i. may ask the individual to provide 2 forms of identification
ii. may contact the individual via phone to confirm the request was made
iii. will respond without delay and within 1 month of receipt of the request (or receipt of the additional information needed to confirm identity; where relevant)
iv. will provide the information free of charge
v. may tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous, or where it is impractical to comply within a month due to school closure. We will inform the individual of this within 1 month and explain why the extension is necessary.

10.3.2 We may not disclose information if it:

i. might cause serious harm to the physical or mental health of the student or another individual
ii. would reveal that the child is being or has been abused, or is at risk of abuse, where the disclosure of that information would not be in the child's best interests
iii. would include another person's personal data that we can't reasonably anonymise, and we don't have the other person's consent and it would be unreasonable to proceed without it
iv. is part of certain sensitive documents, such as those related to crime, immigration, legal proceedings or legal professional privilege, management forecasts, negotiations, confidential references, or exam scripts.

10.3.3 If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs. A request will be deemed to be unfounded or excessive if it is repetitive or asks for further copies of the same information. Should we refuse a request, we will tell the individual why and tell them they have the right to complain to the ICO or they can seek to enforce their subject access rights through the courts.

10.4 Other data protection rights of the individual

10.4.1 In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it, individuals also have the right to:

i. withdraw their consent to processing at any time, where processing is based on the consent of the student or parent
ii. ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
iii. prevent use of their personal data for direct marketing
iv. object to processing which has been justified on the basis of public interest, official authority or legitimate interest
v. object to decisions based solely on automated decision making or profiling ((i.e. making decisions or evaluating certain things about an individual based on their personal data with no human involvement)
vi. be notified of a data breach (in certain circumstances)
vii. make a complaint to the ICO
viii. ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

10.4.2 Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the School's Data Protection Lead who will send it to the DPO for information purposes.

11 Parental/carer requests to see the educational record

11.1 Any requests from parents/carers should be treated as subject access requests in accordance with the above.

12 Closed-Circuit Television (CCTV)

12.1 We use CCTV in various external locations around the school site to ensure it remains safe. We will follow the ICO's guidance for the use of CCTV, and comply with data protection principles. We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded.

Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use. Any enquiries about the CCTV system should be directed to Zak Honah, Proprietor, on Zak@watermelonschools.com.

13 Photographs and videos

13.1 As a School we want to celebrate the achievements of our students and therefore may want to use images and videos of our pupils within promotional materials, or pages in the media such as local, or even national, newspapers covering school events or achievements. The School will obtain written consent from parents/carers, or students aged 18 and over, for photographs and videos to be taken of students for communication, marketing and promotional materials.

13.2 Where the School need parental consent, it shall clearly explain how the photograph and/or video will be used to both the parent/carer and student. Where the School does not need parental consent, it shall clearly explain to the student how the photograph and/or video will be used.

13.3 Uses may include:

i. within the School on notice boards and in School newsletters, magazines, brochures etc.
ii. outside of the School by external agencies such as the newspapers, campaigns etc.
iii. online on our School website or social media pages.

13.4 We do not allow parents / carers to take photographs or video footage at school events.

13.5 Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further. When using photographs and videos in this way, we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

13.6 Please see our Child Protection and Safeguarding Policy and Privacy Policies and Notices for more information on our use of photographs and videos.

14 Data protection by design and default

14.1 Watermelon Independent Schools shall put measures in place to show that it has integrated data protection into all of its data processing activities, including:

i. appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
ii. only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law
iii. completing privacy impact assessments where the School's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
iv. integrating data protection into internal documents including this policy, any related policies and privacy notices
v. training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
vi. regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
vii. maintaining records of our processing activities, including:
    - for the benefit of data subjects, making available the name and contact details of our School and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
    - for all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure

15 Artificial Intelligence (AI)

15.1 Artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard. Watermelon Independent Schools recognises that AI has many uses to help pupils learn, but also poses risks to sensitive and personal data.

15.2 To ensure that personal and sensitive data remains secure, no one will be permitted to enter such data into unauthorised generative AI tools or chatbots.

15.3 If personal and/or sensitive data is entered into an unauthorised generative AI tool, Watermelon Independent Schools will treat this as a data breach, and will follow the personal data breach procedure outlined in appendix 1.

16 Data security and storage of records

16.1 Watermelon Independent Schools will protect personal data and take appropriate security measures against unlawful or unauthorised processing, alteration and disclosure of personal data, and against the accidental or unlawful loss of, destruction or damage.

16.2 The School will put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. All data will be held and disposed of in line with the School's Data Retention and Destruction Policy. In particular:

i. entry controls:
   - Appropriate building security measures such as alarms, window bars and deadlocks
   - Visitors are required to sign in and out and are accompanied

ii. secure lockable desks and cupboards - desks and cupboards should be kept locked if they hold confidential information of any kind (personal information is always considered confidential.)

iii. paper containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice or display boards, or left anywhere else where there is general access

iv. paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use

v. methods of disposal - paper documents should be shredded. Digital storage devices should be physically destroyed when they are no longer required. IT assets must be disposed of in accordance with the ICO guidance on the disposal of IT assets.

https://ico.org.uk/media/for-organisations/documents/1570/it_asset_disposal_for_organisations. pdf

vi. equipment - data users must ensure that individual monitors and projector screens do not show confidential information to passers-by and that they lock access to their screen or log off from their PC when it is left unattended

vii. any device that can be used to access data must be locked if left (even for short periods)

viii. staff must ensure passwords are sufficiently difficult for anyone else to guess by incorporating number, mixed case and special characters and changing them regularly

ix. encryption software is used to protect all portable devices

x. personal data may only be accessed on machines that are securely password protected

xi. standard unencrypted email should never be used to transmit personal or sensitive data.

xii. postal services - where it is necessary to send personal information by post, staff should consider sending personal data by registered mail. Staff should take every opportunity to verify the current address of the recipient to ensure information is sent to the correct address

xiii. internal mail or student post - care should be taken not to send sensitive or personal data home with a student or through an internal mail system

xiv. the use of memory cards, USB memory sticks or other portable storage devices are forbidden. Staff are encouraged to access data remotely through the School's remote desktop facility

xv. Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for school owned equipment (see e safety / acceptable use of ICT policy)

xvi. when personal data is stored on any portable computer system:
   - the data must be encrypted and password protected
   - the device must be encrypted and password protected
   - the device must offer approved virus and malware checking software
   - the data must be securely deleted from the device once it has been transferred or its use is complete

xvii. where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected.

16.3 The School will ensure that IT systems are set up so that access to protected files is denied for unauthorised users and that users will be assigned clearance that will determine which files are accessible to them. Access to protected data will be controlled according to the role of the user. Members of staff will not, as a matter of course, be granted access to the whole management information system.

16.4 The servers and IT infrastructure which forms part of the IT network will be kept in locked rooms and cabinets. Only qualified IT employees or suitably appointed IT contractors may access the physical servers and infrastructure

16.5 Document printing - documents containing personal data must be collected immediately from printers and not left on photocopiers.

16.6 Any member of staff found to be in breach of the above security measures may be subject to disciplinary action.

17 Disposal of records

17.1 Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

17.2 The School will shred paper-based records and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

18 Personal data breaches

18.1 The School shall take all reasonable steps to ensure that there are no personal data breaches. In the unlikely event of a suspected data breach, we will follow the procedure set out in Appendix 1.

18.2 When appropriate, the School shall report the data breach to the ICO within 72 hours after becoming aware of it. Such breaches in a School context may include, but are not limited to:

i. a non-anonymised dataset being published on the School website which shows the exam results of students eligible for the pupil premium
ii. safeguarding information being made available to an unauthorised person
iii. the theft of a School laptop containing non-encrypted personal data about students

19 Training

19.1 All staff and governors are provided with data protection training as part of their induction process. Data protection will also form part of continuing professional development, where changes to legislation, guidance or the School's processes make it necessary.

20 Changes to this policy

Watermelon Independent Schools may change this policy at any time. Where appropriate, we will notify data

subjects of those changes. The DPL is responsible for monitoring and reviewing this policy. This policy will be reviewed annually and approved by the proprietor.

Appendix 1: Personal data breach procedures

If staff become aware that information has not been handled according to procedures and there is a data breach or potential security incident, they must report it in accordance with this procedure.

When appropriate, the School will report the data breach to the ICO within 72 hours in accordance with the requirements of the GDPR.

Data protection breaches occur where personal data is lost, damaged, destroyed, stolen, misused and/or accessed unlawfully.

Examples of how a breach may occur include:

Theft of data or equipment on which data is stored
Loss of data or equipment on which data is stored
Inappropriate access controls allowing unauthorised use
Accidental Loss
Destruction of personal data
Damage to personal data
Equipment failure
Unlawful disclosure of personal data to a third party
Human error
Unforeseen circumstances such as fire or flood
Hacking attack
'Blagging' offences where information is obtained by deceiving the organisation which holds it.

If any member of staff of the School, or a director discovers that data has been lost, or believes that there has been a breach of the data protection principles in the way that data is handled, they must immediately or no later than within 24 hours of first coming to notice, inform the School's designated Data Protection Officer.

Upon being notified, the School's designated Data Protection Officer will assess whether a breach of personal information has occurred, and the level of severity. If a breach has occurred but the risk of harm to any individual is low (for example, because no personal information has left the control of the School, then the School's Data Protection Officer will undertake an internal investigation to consider whether the Information Security Policy was followed, and whether any alterations need to be made to internal procedures as a result.

In all other cases, the incident must be notified to the Data Protection Officer immediately, who must follow the Information Commissioner's Office guidelines on notification and recording of the breach. The priority must then be to close or contain the breach to mitigate / minimise the risks to those individuals affected by it.

All School staff and directors are expected to work in partnership with the designated Data Protection Officer in relation to the following matters.

Notification of Breaches

Any member of staff or proprietor who becomes aware of a personal information breach should provide full details to the designated Data Protection Officer for the School within 24 hours of being made aware of the breach. The Data Protection Officer will then complete the Data Breach Record Form and Incident Log. When completing the form, details should be provided of the reporter's name, the date/time of the breach, the date/time of detecting the breach, and basic information about the type of breach and information about personal data concerned. Details of what has already been done to respond to the risks posed by the breach should also be included.

Containment and Recovery

The initial response is to investigate and contain the situation and a recovery plan including damage limitation. The school may need input from specialists such as IT, HR and legal and in some cases contact with external third parties.

The school should:

- Seek assistance in the containment exercise. This could be isolating or closing a compromised section of the network, recovery of released documents, finding a lost piece of equipment or simply changing any related access codes
- Establish whether there is anything you can do to recover any losses and limit the damage the breach can cause.
- As well as the physical recovery of equipment, this could involve the use of backup records to restore lost or damaged data or ensuring that staff recognise when someone tries to use stolen data to access accounts.
- Consider whether any individual affected by the data breach should be notified

Assessing the Risks

Levels of risk can be very different and vary on an individual breach of data security depending on what is lost/damaged/stolen. For example, if a case file is lost then risks are different depending on type of data and its sensitivity with potential adverse consequences for individuals. The designated Data Protection Officer should consider the following points:

- What type of data is involved?
- How sensitive is the data?
- If data has been lost or stolen, are there any protections in place such as encryption?
- What has happened to the data?
- If data has been stolen, could it be used for purposes which are harmful to the individuals to whom the data relate? If it has been damaged, this poses a different type and level of risk.
- Regardless of what has happened to the data, what could the data tell a third party about the individual? Sensitive data could mean very little to an opportunistic laptop thief while the loss of apparently trivial snippets of information could help a determined fraudster build up a detailed picture of other people
- How many individuals' personal data has been affected by the breach?
- Who are the individuals whose data has been breached?
- What harm can come to those individuals?
- Are there risks to physical safety or reputation, of financial loss or a combination of these and other aspects of their life?
- Are there wider consequences to consider such as a risk to life?
- Loss of public confidence in the School?

All staff and proprietor(s) establish whether there is anything they can do to recover any losses and limit the damage the breach can cause.

Appendix 2: Personal data breach log and incident reporting for

Personal Data Security Breach Organisation: Watermelon Independent Schools

Personal Data Security Breach – Incident Reporting Form

NO.	REF	Date/time of incident	This form should be used to provide information to the Data Protection Officer when there has been a *serious* breach and consideration needs to be given to whether the breach should be reported to the ICO. The aim of the form is to gather detailed information in order to understand the gravity of the breach, including its impact and what must be done to reduce the risk to personal data and the individuals concerned. It is imperative that as much information as possible is provided. The information will be used to review policies and procedures and assess whether changes are required. Breach log no: _____ Breach log reference: _____	S TAKEN/ TO BE TAKEN?		
				e the ected ata jects een med?	Has the DPO been informed?	Does the breach need to be reported to the ICO?

1. Details of the breach

a) Date and Time of the Incident

b) Number and description of individuals whose data is affected (eg 3 year 10 pupils)

c) Department (if relevant)