Poole High School

VALUED • INSPIRED • EMPOWERED

DATA HANDLING POLICY

Staff Link:	P Myers	**Date:**	July 2019
Governor Link:	P Woodroffe	**First Review:**	July 2021
		Subsequent Reviews:	Bi-annual

1. Introduction - Awareness

Schools should do everything within their power to ensure the safety and security of any material of a personal or sensitive nature.

It is the responsibility of all members of the school community to take care when handling, using or transferring personal data that it cannot be accessed by anyone who does not:

- **have permission to access that data**
- **need to have access to that data.**

Any loss of personal data can have serious effects for individuals and / or institutions concerned, can bring the school into disrepute and may well result in disciplinary action and / or criminal prosecution. All transfer of data is subject to risk of loss or contamination.

Anyone who has access to personal data must know, understand and adhere to this policy, which brings together the legal requirements contained in relevant data legislation and relevant regulations and guidance from the Local Authority.

The General Data Protection Regulation (GDPR) lays down a set of rules for processing of personal data (both structured manual records and digital records). It provides individuals (data subjects) with rights of access and security and requires users of data (data processors) to be open about how it is used and to follow "good information handling principles".

1.1 Policy Statements

Article 5 of the GDPR requires that personal data shall be:

- processed lawfully, fairly and in a transparent manner in relation to individuals;
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals;

- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

As such the school undertakes to hold the minimum personal information necessary to enable it to perform its function and information will be erased once the need to hold it has passed for students this is when they reach the age of 25 (School leaving age +7 years). See Appendix A for the retention schedule.

Every effort will be made to ensure that information is accurate, up to date and that inaccuracies are corrected without unnecessary delay. We will send data checking forms annually but parents can make amendments as often as they like.

All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing".

1.2 Information to Parents / Careers – the "Privacy Notice" Appendix

Under the "Fair Processing" requirements in the GDPR the school will inform parents/carers of all students of the data they hold on the pupils / students, the purposes for which the data is held and the third parties (e.g. LA, DCSF, QCA, Connexions etc.) to whom it may be passed. This fair processing notice will be passed to parents/carers through the home-school agreement and on the website.

2. Information we hold and why we hold it.

2.1 Personal Data

The school will have access to a wide range of personal information and data. The data may be held in digital format or on paper records. Personal data is defined as any combination of data items that identifies an individual and provides specific information about them, their families or circumstances. Access to data is restricted so that only members of the school community who need access will be able to access it.

The information we collect will include:

Personal information about members of the school community:

For students we collect and process data relating to the students on roll (and formerly on roll).This information will include their

- contact details,
- national curriculum assessment results,
- attendance information,
- any exclusion information,
- where they go after they leave us,

and personal characteristics such as their

- ethnic group,
- any special educational needs
- relevant medical information.

For students enrolling for post 14 qualifications, the Learning Records Service will give us the unique learner number (ULN) and may also give us details about their learning or qualifications.

Once our students reach the age of 13, the law requires us to pass on certain information to the Borough of Poole or the Youth Support Services in the area (Connexions) who have responsibilities in relation to the education or training of 13-19 year olds. We may also share certain personal data relating to young people aged 16 and over with post-16 education and training providers in order to secure appropriate services for them.

A parent/carer/guardian can request that **only** their child's name, address and date of birth be passed to Borough of Poole or Youth Support Services by informing the school. This right is transferred to the young person once they reach the age of 16. For more information about services for young people, please go to our local authority website at www.poole.gov.uk/communities-and-people/youth-support/youth-service.

We share data (for the purposes of providing systems) with the following companies as data processors. In principle the purposes of these systems are to support the core principles of the school by providing accounts and tracking progress.

Data Processor	Reason	Information shared.
E-praise.co.uk	To provide login details Facilitate tracking and classroom management	Name, DoB, Class information, House, Gender, UPN, Year Group, AEN, Pupil Premium, EAL and Child in Care information
Capita SIMS – our Management Information System providers.	To provide login details For resolving issues.	Parent names and related student information are provided to create logins. Under normal circumstances they have no access to personal data, but may be allowed access in the event of a problem with the Management Information system. In this case, this is carried out over an encrypted link and data is retained only so long as it is needed to resolve the issue.
Google – providers of email and online storage system	To provide login details	Name, Year Group, Class information, House, UPN, Year Group.
GCSEPod	To provide login details	Name, Year Group, Class information, House, UPN, Year Group.
Accelerated Reader	To provide login details	Name, DoB, Timetable information, Ethnicity, AEN
Kerboodle	To provide login details	Name, DoB, Class Information.
Wonde	To transfer data to other processors. They are a conduit but do not actually do any processing of the data.	Name, DoB, Class information, House, Gender, UPN, Year Group, AEN, Pupil Premium, EAL and Child in Care information
GroupCall	To transfer data to other processors. They are a conduit but do not actually do any processing of the data.	Name, DoB, Class information, House, Gender, UPN, Year Group, AEN, Pupil Premium, EAL and Child in Care information

We will not give information about our pupils to anyone without your consent (as indicated via the Data Collection Form parents/carers/guardians complete on entry to the school) unless the law and our policies allow us to do so.

If you want to receive a copy of the information about your child that we hold, please contact school@poolehigh.poole.sch.uk in the first instance.

We are required, by law, to pass some information about our students to the Department for Education (DfE). This information will, in turn, then be made available for use by the Local Authority.

The DfE may also share student level personal data that we supply to them, with third parties. This will only take place where legislation allows it to do so and it is in compliance with the GDPR from May 2018.

Decisions on whether DfE releases this personal data to third parties are subject to a robust approval process and are based on a detailed assessment of who is requesting the data, the purpose for which it is required, the level and sensitivity of data requested and the arrangements in place to store and handle the data. To be granted access to student level data, requestors must comply with strict terms and conditions covering the confidentiality and handling of data, security arrangements and retention of use of the data.

For more information on how this sharing process works please visit:
https://www.gov.uk/guidance/national-pupil-database-apply-for-a-data-extract.

For information on which third party organisations (and for which project) student level data has been provided to, please visit: https://www.gov.uk/government/publications/national-pupil-database-requests-received .

If you need more information about how our local authority and/or DfE collect and use your information, please visit:

- https://poole.gov.uk (Our local authority)

- https://www.gov.uk/data-protection-how-we-collect-and-share-research-data (DfE)

If you are unable to access these websites, please contact the DfE as follows: Public Communications Unit, Department for Education, Sanctuary Buildings, Great Smith Street, London SW1P 3BT

For staff members we collect and process data which will include their

- Personal details such as
    - names,
    - addresses,
    - contact details,
    - contact details,
    - disciplinary records
- Professional records e.g.
    - employment history,
    - training
    - taxation and national insurance records,
    - appraisal records
    - absence Information

- references
-

Data Processor	Reason	Information shared.
Dorset Payroll	To provide payroll services	Name, Bank details,
Capita SIMS	For troubleshooting and problem resolution	Personnel Record as held in sims
SBS	For HR and consultancy	Name, payscale, hours worked, employee number, start date, dates for maternity leave (if applicable), leaving date.
Occupational Health	Ad hoc	Name, reason for referral
Potential Future employers	References	Name, Current Position, attendance summary, performance summary, safeguarding information.
E-praise.co.uk	To provide login details Facilitate tracking and classroom management	Name, email, Class information
Capita SIMS – our Management Information System providers.	To provide login details For resolving issues.	Name, Email address are provided to create logins. Under normal circumstances they have no access to personal data, but may be allowed access in the event of a problem with the Management Information system. In this case, this is carried out over an encrypted link and data is retained only so long as it is needed to resolve the issue.
Google – providers of email and online storage system	To provide login details	Name, MIS id, Class information, Staff code.
GCSEPod	To provide login details	Name, Email Address, class information.
Accelerated Reader	To provide login details	Name, Email Address
Kerboodle	To provide login details	Name, email address.
Wonde	To transfer data to other processors. They are a conduit but do not actually do any processing of the data.	Name, payscale, hours worked, employee number, start date, dates for maternity leave (if applicable), leaving date.
GroupCall	To transfer data to other processors. They are a conduit but do not actually do any processing of the data.	Name, DoB, Class information, House, Gender, UPN, Year Group, AEN, Pupil Premium, EAL and Child in Care information

2.1 Data Protection Officers

Registration

The school is registered as a Data Controller on the Data Protection Register held by the Information Commissioner. The registration number is Z890387X and the most up to date register entry can be seen at: https://ico.org.uk/ESDWebPages/Entry/Z890387X

Responsibilities

The school's Data Protection Officer is Handsam Ltd. (https://www.handsam.education/) and can be contacted at info@handsam.co.uk..The school's Senior Information Risk Officer (SIRO) is Peter Myers. He will keep up to date with current legislation and guidance and will:

- determine and take responsibility for the school's information risk policy and risk assessment
- appoint the Information Asset Owners (IAOs)

The school has identified Information Asset Owners (IAOs) for the various types of data being held (e.g. student information / staff information / assessment data etc.). The IAOs will manage and address risks to the information and will understand:

- What information is held and for what purpose
- Who has access to protected data and why

IAO	Type of Data	Why
Finance Staff	Financial	Job Function
Staffing Officer	Personnel	Job Function
Operations Manager	Financial and Personnel	Job Function
Pastoral and Attendance Officers	Student	Job Function
Heads of Year and Progress Leaders	Student	Job Function
Head of IT and Data Security	All	SIRO Job Function
Catering Manager/Staff	Limited Financial and Student	Job Function
Head teacher	All	Job Function
Deputy Head teacher	All	Job Function (in absence of Head Teacher)
Data Manager	Assessment, Student	Job Function
Teacher	Assessment , Registration, Limited student	Job Function
Grounds	CCTV	Job Function
LSAs	Assessment , Registration, Limited student	Job Function
Admin	Student	Job Function
HT PA	Student, Personnel	Job Function
DHT PA	Student	Job Function
HoDs	Limited Personnel (Performance Management)	Job Function
IT Technicians	Student, Limited Staff.	Job Function

Everyone in the school has the responsibility of handling protected or sensitive data in a safe and secure manner.

Governors are required to comply fully with this policy in the event that they have access with personal data, when engaged in their role as a Governor.

2.2 Lawful basis for processing personal data

We collect and hold personal information relating to our students and may also receive information about them from their previous school and/or local authority and/or Department for Education (DfE). We use this personal data to:

- support our students' learning;
- monitor and report on their progress;
- provide appropriate pastoral care; and
- assess the quality of our services.

The legal basis for our processing or personal data have been identified in 6 areas:

Contractual necessity	Personal data may be processed on the basis that such processing is necessary in order to enter into or perform a contract with the data subject.	The school cannot function without basic information relating to the individuals it is educating.
Compliance with legal obligations	Personal data may be processed on the basis that the controller has a legal obligation to perform such processing.	We are required to keep certain records and submit them to government (e.g. School Census information or reporting a safeguarding concern to children's services.)
Substantial Public interest	Personal data may be processed on the basis that such processing is necessary for the performance of tasks carried out by a public authority or private organisation acting in the public interest.	• Providing students with an education. • Safeguarding and promoting students' welfare • Ensuring that all relevant legal obligations of the school are complied with. • Promoting the objects and interests of the school. • Facilitating the efficient operation of the school.
Vital Interests	Personal Data may be processed on the basis that it is necessary for the establishment to protect the vital interests of a data subject	If a person were to be seriously hurt or unconscious the school would share medical information.
Consent	Personal data may be processed on the basis that the data subject has consented to such processing. Parental permission is required to process the personal data of children (and note that a child is anyone under the age of 16). In some contexts (especially online) proving that parental	We seek parental consent for processing of data and use this as a final basis. The parental consent will be used for example to allow or deny the use of photographs of students. We will still collect basic information and use it under the above criteria. We will not use any

	permission has been obtained may be difficult.	data outside of the criteria above if we cannot obtain consent.

2.3 Consent

A consent form is sent to parents to sign when their child starts at the school. This encompasses not just data protection but also medical release and other similar consents. We break the consent for media use into several categories (in school, website, social media, staff training) and also seek the students' permission for using their image in addition. Where there is a conflict in permissions the student's permissions take precedent, unless they are under the age of 13 when the parents would.

A parent/carer/guardian can request that **only** their child's name, address and date of birth be passed to Borough of Poole or Youth Support Services by informing the school. This right is transferred to the young person once he reaches the age of 16. For more information about services for young people, please go to our local authority website at www.poole.gov.uk/communities-and-people/youth-support/youth-service. This option is indicated on the data collection forms.

We will not give information about our pupils to anyone without your consent (as indicated via the Student Information Form parents/guardians complete on entry to the school) unless the law and our policies allow us to do so.

If you want to receive a copy of the information about your child that we hold, please contact school@poolehigh.poole.sch.uk in the first instance and ask to make a Subject Access Request.

2.4 Training & awareness

All staff will receive data handling awareness / data protection training and will be made aware of their responsibilities, as described in this policy through:

- Induction training for new staff
- Staff meetings / briefings / Inset
- Notifications as part of the digital signage in the staffroom.
- Day to day support and guidance from Information Asset Owners

2.5 Risk Assessments

Information risk assessments will be carried out by Information Asset Owners to establish the security measures already in place and whether they are the most appropriate and cost effective. The risk assessment will involve:

- Recognizing the risks that are present
- Judging the level of the risks (both the likelihood and consequences)
- Prioritizing the risks

2.6 Impact Levels and protective marking

The school will ensure that all school staff, contractors working for it, and delivery partners, comply with restrictions applying to the access to, handling and storage of data classified as Protect, Restricted or higher. Unmarked material is considered 'unclassified'. The term 'UNCLASSIFIED' or 'NON' or 'NOT PROTECTIVELY MARKED' may be used to indicate positively that a protective marking is not needed.

All documents (manual or digital) that contain protected or restricted data will be labelled clearly with the Impact Level (Protect or Restrict) shown in the header and the Release and Destruction classification (Securely delete or shred this information when you have finished using it) in the footer.

Users must be aware that when data is aggregated the subsequent impact level may be higher than the individual impact levels of the original data. Combining more and more individual data elements together in a report or data view increases the impact of a breach. A breach that puts a learner at serious risk of harm will have a higher impact than a risk that puts a learner at low risk of harm. Breaches that may lose any party lots of money have a higher impact than losses of a few pounds. Long-term significant damage to anyone's reputation has a higher impact than damage that might cause short-term embarrassment.

2.7 Secure Storage of and access to data

The school will ensure that ICT systems are set up so that the existence of protected files is hidden from unauthorised users and that users will be assigned a 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, for example staff data is available to the Staffing Officer and their substitutes, SLT and Head of IT and Data Security/Senior ICT Technician. Access to student records is extended to teaching staff and those members of staff (LSA's, House Officers, teachers) who need access. Financial information is restricted to the Finance department, Operations Manager, Head and Deputy plus Head of IT and Data Security/Senior ICT Technician (for maintenance and troubleshooting purposes).

All users will be given secure user names and strong passwords which must be changed regularly. Details are in the Password Policy. User names and passwords must never be shared.

Personal data may only be accessed on machines that are securely password protected. Any device that can be used to access data must be locked if left (even for very short periods) and set to auto lock.
All storage media must be stored in an appropriately secure and safe environment that avoids physical risk, loss or electronic degradation.

Personal data can only be stored on school equipment (this includes computers and portable storage media). Private equipment (i.e. owned by the users) must not be used for the storage of personal data.
When personal data is stored on any portable computer system, USB stick or any other removable media:

- the data must stored on encrypted media only.
- the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete

The school has clear policy and procedures for the automatic backing up, accessing and restoring all data held on school systems, including off-site backups.

All paper based Protected and Restricted (or higher) material must be held in lockable storage.

3.Right of Access

The school recognises that under Article 15 of the General Data Protection Regulation, data subjects have a number of rights in connection with their personal data, the main one being the right of access. Procedures are in place to deal with Subject Access Requests i.e. a written request to see all or a part of the personal data held by the data controller in connection with the data subject. Data subjects have the right to know: if the data controller holds personal data about them; a description of that data; the purpose for which the data is processed; the sources of that data; to whom the data may be disclosed; and a copy of all the personal data that is held about them. Under certain circumstances the data subject can also exercise rights in connection with the rectification; blocking; erasure and destruction of data.

4: Data breaches

4.1 What constitutes a data breach?

A data breach occurs when Personal Data is put at risk of exposure, or is exposed beyond its intended use by authorised personnel, e.g.

- Failure to lock a computer and office when leaving the room allowing students to access sims.
- Leaving a trip register on a coach giving personal student data to the coach driver or future passengers.
- Leaving an AIL folder in a classroom allowing a visitor to steal personal data.
- Not locking a filing cabinet containing student files
- Leaving encryption key plugged into your laptop allowing a thief to access personal data on the hard drive.
- Keeping your encryption key with your laptop allowing a thief to access personal data on the hard drive.
- Sharing username and password details with other users
- Allowing unauthorised users, e.g. family members to use school IT equipment.

These are just examples to demonstrate the type of instance but this list should not considered definitive and are not limited to this list.

There is a legal requirement to report any instance of a data breach immediately. The ICO must be informed within 72 hours of the breach occurring. Failure to do so puts both the individual and the school at risk of prosecution for non-disclosure.

Failure to take proper steps to secure all data could result in disciplinary action under the schools prevailing disciplinary policy.

4.2 What happens in the event of a data breach?

The member of staff responsible for monitoring and managing breaches of information security,

e.g. the school's designated Information Security Officer, should immediately implement the school's information breach management plan once an incident is reported to them. The responsible officer should work with relevant managers and specialists, e.g. ICT or communications specialists, at each step of the process.

There are 2 principal methods for a data breach occurring:

a. Loss of data (e.g. leaving a folder on a bus).
b. Breach of Security (Physical or IT) (where someone has actually forced entry to access data).

However the breach has occurred, there is a breach management plan composed of four important elements. This must be considered immediately by the Information Security Officer together with the relevant line manager:

- Assessment of ongoing risk
- Containment and recovery
- Notification of breach
- Evaluation and response

4.2.1 Assessing the risks

Assess the risks that may be associated with the breach. Most important is an assessment of potential adverse consequences for individuals, how serious or substantial these are and how likely they are to happen. Risk assessment includes a classification of the incident.

4.2.1.1 Incident Classification

Incidents should be classified according to severity of risk, as follows:

Level	Severity of Risk
1	• High risk of harm to individuals whose confidentiality has been breached. • High risk of embarrassment to the school, including press coverage.
2	• Intermediate risk of harm to individuals whose confidentiality has been breached. • Intermediate risk of embarrassment to the school
3	• Low risk of harm to individuals whose confidentiality has been breached. • Low risk of risk of embarrassment to the school

NOTE: Incident classification will depend on school policy on the level of sensitivity ascribed to personal or other types of information. Although name, address and date of birth are generally considered to be confidential but not highly sensitive, in certain circumstances these may be considered to be sensitive. Sensitivity of information will also depend on the personal circumstances of the individuals concerned, e.g. a child looked after by the local authority.

Examples can be seen in Appendix C

All breaches of information security must be treated seriously and reported according to agreed school procedure.

Discovery of illegal material within the school's network or other illegal activities must be reported at once to the police. Do not do anything to the suspect computer/s or other equipment, including turning on or off, or shut down the network unless instructed to do so by the Police. Do not attempt to conduct your own investigation or bring an outside expert to do so as this may compromise the evidence if a legal case were to result.

4.2.1.2 Containment and recovery

Information security breaches will require not just an initial response to investigate and contain the situation but also a recovery plan including, where necessary, damage limitation. This will often involve input from specialists across the school and East Sussex County Council such as ICT and human resources, and in some cases contact with external stakeholders and suppliers.

For Level 1 and some Level 2 incidents, schools may also need to seek legal advice. In case of pupil or staff involvement in illegal activities, the school should take legal advice as soon as possible, particularly with regard to acceptable disciplinary actions while the police are carrying out their investigation.

4.2.1.3 Notification of breaches

Informing people and organisations that the school has experienced an information security breach is an important element of the breach management plan. However, informing people about a breach is not an end in itself. Notification should have a clear purpose, whether this is to enable individuals who may have been affected to take steps to protect themselves or to provide advice and deal with complaints.

If the security incident involved pupils, e.g. the breach involved pupils' personal information, pupils witnessed inappropriate material, a pupil was responsible for the incident, etc, the relevant parents must be informed as soon as the incident has been fully investigated to establish facts and containment and recovery measures have been put in place. In some situations, it may be necessary to inform pupils and parents as soon as the incident is discovered, if there is cause to believe that the pupils' personal safety is at immediate risk.

If the incident involved the personal information about a looked after child or the incident is likely to cause harm to a looked after child, e.g. if the child is the victim of cyberbullying or stalking, the school should inform the relevant local authority immediately.

4.2.4 Evaluation and response

Schools should keep a log of all security incidents and monitor all such incidents regularly, allowing for any trends to be picked up and preventative measures to be put in place.

It is important not only to investigate the causes of the breach but also to evaluate the effectiveness of the response to it. If the breach was caused, even in part, by systemic and ongoing problems, then simply containing the breach and continuing 'business as usual' is not acceptable.

If the response was hampered by inadequate policies or a lack of a clear allocation of responsibility then it is important to review and amend these in light of the weaknesses identified.

If the security incident was caused by pupils or staff in direct contravention of school policies, procedures or guidance, the school should take appropriate disciplinary action. The action taken will depend on the severity of risk and the risk classification level ascribed to the incident, i.e. whether the incident is Level 1, 2 or 3.

The school should debrief staff and pupils after the incident in order to maximise what can be learnt.

5: Processing, Storage and Transfer of data

5.1 Processing of personal data

All personal data will be processed in accordance with the terms of the GDPR. Where processing procedures are changed then a data protection impact assessment is undertaken.

5.1 Secure transfer of data and access out of school

The school recognises that personal data may be accessed by users out of school, or transferred to the LA or other agencies. In these circumstances:

- Users may not remove or copy sensitive or personal data from the school or authorised premises without permission and unless the media is encrypted and password protected and is transported securely for storage in a secure location.
- Users must take particular care that computers or removable devices which contain personal data must not be accessed by other users (e.g. family members) when out of school.
- When sensitive or personal data is required by an authorised user from outside the organisation's premises (for example, by a member of staff to work from their home), they should preferably have secure remote access to the management information system or learning platform
- If secure remote access is not possible, users must only remove or copy personal or sensitive data from the organisation or authorised premises if the storage media, portable or mobile device is encrypted and is transported securely for storage in a secure location
- Users must protect all portable and mobile devices, including media, used to store and transmit personal information using approved encryption software.
- Particular care should be taken if data is taken or transferred to another country, particularly outside Europe, and advice should be taken from the local authority in this event.

5.2 Disposal of data

The school will comply with the requirements for the safe destruction of personal data when it is no longer required.

The disposal of protected data, in either paper or electronic form, must be conducted in a way that makes reconstruction highly unlikely. Electronic files must be securely overwritten, in accordance with government guidance, and other media must be shredded, incinerated or otherwise disintegrated for data.

A Destruction Log should be kept of all data that is disposed of. The log should include the document ID, classification, date of destruction, method and authorisation.

5.3 Audit Logging / Reporting / Incident Handling

It is good practice, as recommended in the "Data Handling Procedures in Government" document that the activities of data users, in respect of electronically held personal information, will be logged and these logs will be monitored by responsible individuals. (insert name or title)

The audit logs will be kept to provide evidence of accidental or deliberate security breaches – including loss of protected data or breaches of an acceptable use policy, for example.

The school has a policy for reporting, managing and recovering from information risk incidents, which establishes:

- a "responsible person" for each incident
- a communications plan, including escalation procedures and results in a plan of action for rapid resolution and
- a plan of action of non-recurrence and further awareness raising.

All significant data protection incidents must be reported through the SIRO to the Information Commissioner's Office based upon the local incident handling policy and communication plan.

Appendix A Retention Schedule

Appendix B Use of Technologies and Protective Marking

	The information	The technology	Notes on Protect Markings (Impact Level)
School life and events	School terms, holidays, training days, the curriculum, extra-curricular activities, events, displays of pupils work, lunchtime menus, extended services, parent consultation events	Common practice is to use publically accessible technology such as school websites or portal, emailed newsletters, subscription text services	Most of this information will fall into the NOT PROTECTIVELY MARKED (Impact Level 0) category.
Learning and achievemen t	Individual learner's academic, social and behavioural achievements, progress with learning, learning behaviour, how parents can support their child's learning, assessments, attainment, attendance, individual and personalised curriculum and educational needs.	Typically schools will make information available by parents logging on to a system that provides them with appropriately secure access, such as a Learning Platform or portal, or by communication to a personal device or email account belonging to the parent.	Most of this information will fall into the PROTECT (Impact Level 2) category. There may be learners whose personal data requires a RESTRICTED marking (Impact Level 3) or higher. For example, the home address of a child at risk. In this case, the school may decide not to make this learners record available in this way.
Messages and alerts	Attendance, behavioural, achievement, sickness, school closure, transport arrangements, and other information that it may be important to inform or contact a parent about as soon as possible. This may be particularly important when it is necessary to contact a parent concerning information that may be considered too sensitive to make available using other online means.	Email and text messaging are commonly used by schools to contact and keep parents informed. Where parents are frequently accessing information online then systems e.g. Learning Platforms or portals, might be used to alert parents to issues via "dashboards" of information, or be used to provide further detail and context.	Most of this information will fall into the PROTECT (Impact Level 1) category. However, since it is not practical to encrypt email or text messages to parents, schools should not send detailed personally identifiable information. General, anonymous alerts about schools closures or transport arrangements would fall into the NOT PROTECTIVELY MARKED (Impact Level 0) category.

Appendix C: Examples of incidents (not exhaustive)

Level 1 – High risk of harm to individuals or embarrassment to school

- Highly sensitive information about one or more pupils held on unencrypted USB memory stick or laptop or paper left on public transport or stolen from car
- Highly sensitive information about one or more pupils sent to wrong fax number or address
- Confidential information, even if not highly sensitive, about 5 or more pupils left on public transport or stolen from car or sent to wrong fax number or address
- Address of a child in local authority care is disclosed to his birth parents when they are not supposed to know (the local authority has notified that the school should not disclose address)
- Discovery of indecent images of children within the school network (see below for dealing with illegal activity)

Level 2 -Intermediate risk of harm to individuals or embarrassment to school

- Confidential information, which is not highly sensitive, about 1 to 5 pupils held on unencrypted USB memory stick or laptop or paper left on public transport or stolen from car (but please see note above)
- Staff members sharing passwords
- Staff accessing database in advance of authority to do so or without the need to know
- A pupil deliberately accessing, printing and showing inappropriate material or inadvertently accessing such material but subsequently showing to other pupils

Level 3 – Low risk of harm to individuals or embarrassment to the school

- Loss or misplacement of information within school premises
- A pupil inadvertently accessing inappropriate material without subsequently showing it to others and reporting to teacher about the access
- Pupils sharing passwords

Appendix D Notes for Staff

It is the responsibility of all members of the school community to take care when handling, using or transferring personal data that it cannot be accessed by anyone who does not:

- have permission to access that data
- need to have access to that data.

This might, for example mean ensuring that SIMS Learning Gateway is not accessible on a home computer by virtue of a saved password. It could equally mean not leaving papers containing personal data unsupervised in a classroom or on a table at home.

Any loss of personal data can have serious effects for individuals and / or institutions concerned, can bring the school into disrepute and may well result in disciplinary action and / or criminal prosecution. All transfer of data is subject to risk of loss or contamination.

Staff must therefore take all possible precautions to ensure the security and integrity of the data that the school holds.

This includes, but is not limited to:

- Locking all computers which may have access to personal data when leaving them.
- Only having copies of personal data required.
- Storing electronic copies only on secure encrypted devices
- Disposing of paper copies of personal data in the confidential waste sacks which will then be disposed of securely when full.
- Changing their passwords regularly
- Never sharing their usernames and passwords.
- Restricting the storage of personal information to school devices (e.g. not transferring data to a personal computer.
- Paper based records must be stored securely during their lifetime.

It is also important to note that any records relating to somebody's personal data must be disclosed under freedom of subject access requests. It is important therefore to record everything is a proper manner and remember that any record may be viewed at a later date.

Impact Levels and protective marking

The school will ensure that all school staff, contractors working for it, and delivery partners, comply with restrictions applying to the access to, handling and storage of data classified as Protect, Restricted or higher. Unmarked material is considered 'unclassified'. The term 'UNCLASSIFIED' or 'NON' or 'NOT PROTECTIVELY MARKED' may be used to indicate positively that a protective marking is not needed.

All documents (manual or digital) that contain protected or restricted data will be labelled clearly with the Impact Level It is good practice for this to be shown in the header and the Release and Destruction classification in the footer.

Remember when data is aggregated the subsequent impact level may be higher than the individual impact levels of the original data. Combining more and more individual data elements together in a report or data view increases the impact of a breach. A breach that puts a learner at serious risk of harm will have a higher impact than a risk that puts a learner at low risk of harm. Breaches that may lose any party lots of money have a higher impact than losses of a few pounds. Long-term significant damage to anyone's reputation has a higher impact than damage that might cause short-term embarrassment.

Release and destruction markings should be shown in the footer e.g. “Securely delete or shred this information when you have finished using it”.