DATA PROTECTION POLICY

1.0	6.12.2016	Data Protection Policy Agreed Horizon Multi Academy Trust
Version	**Date**	**Description**

1. Introduction

1.1. Statement

The Horizon Multi Academy Trust and their employees should do everything reasonable possible to ensure the safety and security of any material of a personal or sensitive nature.

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

- have permission to access that data, and/or
- need to have access to that data.

Data breaches can have serious effects on individuals, school and the whole academy concerned.

It can bring the school into disrepute and may well result in disciplinary action, criminal prosecution and fines imposed by the Information Commissioners Office . for the school and the individuals involved. All transfer of data is subject to risk of loss or contamination.

1.2. Aim and purpose

This policy provides guidelines that must be followed in relation to data protection.

1.3. Who it applies too

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 protection legislation and relevant regulations and guidance.

2. Policy

2.1. Description

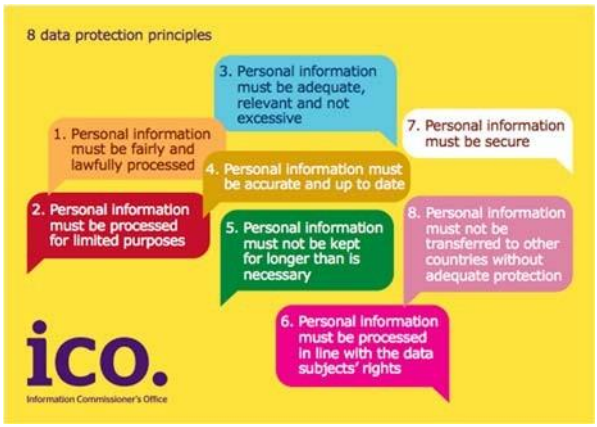
The school will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.

Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.

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

8 Data Protection Principles

The Horizon Multi Academy Trust adhere to the 8 data protection principles outlined by the Information Commissioner's office. These are illustrated on the picture (right). The guidelines within this section cover these principles as required.



Personal Data

The school and individuals will have access to a wide range of personal information and data. The data may be held in a 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. This will include but is not limited to:

- Personal information about members of the school community – including pupils/students, members of staff and parents/carers eg names, addresses, contact details, legal guardianship contact details, health records, disciplinary records
- Curricular/academic data e.g. class lists, pupil/student progress records, reports, references
- Professional records eg employment history, taxation and national insurance records, appraisal records and references
-

Any other information that might be disclosed by parents/carers or by other agencies working with families or staff members.

Registration

The academy is registered as a Data Controller on the Data Protection Register held by the Information Commissioner.

Information to Parents/Carers – the "Privacy Notice"

In order to comply with the fair processing requirements of the DPA, the school will inform parents/carers of all pupils/students of the data they collect, process and hold on the pupils/students, the purposes for which the data is held and the third parties (eg LA, DfE, etc) to whom it may be passed. This privacy notice will be passed to parents/carers through regular forms of communications including text, newsletters and parent meetings. See Appendix 2.

Training & awareness

All staff will receive annual 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
Day to day support and guidance from Information Asset Owners

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:

Recognising the risks that are present;
Judging the level of the risks (both the likelihood and consequences); and
Prioritising the risks.

Risk assessments are an ongoing process and should result in the completion of an Information Risk Actions Form which will be held centrally on the WHFIT Support Teams service desk.

Impact Levels and protective marking

Following incidents involving loss of data, the Government recommends that the Protective Marking Scheme should be used to indicate the sensitivity of data. The Horizon Multi Academy Trustwill follow the Impact Levels as follows:

The Horizon Multi Academy Trust Marking Scheme	Impact Level (IL)	Release and Destruction Classification.
NOT PROTECTIVELY MARKED	0	None
CONFIDENTIAL	1	Securely shredded or
HIGHLY CONFIDENTIAL	2	Securely shredded or

The school will ensure that all school staff, independent 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 '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 shown in the header and the Release and Destruction classification 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 students/pupils at serious risk of harm will have a higher impact than a risk that puts them at low risk of harm. Long-term significant

damage to reputation has a higher impact than damage that might cause short-term embarrassment.

Release and destruction markings should be shown in the footer eg. "Securely delete or shred this information when you have finished using it".

Secure Storage of and access to data

The Horizon Multi Academy Trust will set up ICT systems that the existence of protected files is hidden from unauthorised users. 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 unless this has been agreed by the principal of the school.

Users will use strong passwords which must be changed regularly in accordance with the Password policy. 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 sensitive data must be locked if left (even for very short periods) and reasonable steps taken to prevent unauthorised access.

All storage media must be stored in an appropriately secure and safe environment that avoids physical risk, loss or electronic degradation.

If staff members use a USB or removable hard drive for confidential data it must be encrypted. Network policies will be put into place enforcing only the use of encrypted devices for staff. If staff use a laptop which leaves the school premises containing confidential data this will also be encrypted and a start-up pin assigned to the device.

Personal data should only be stored on school equipment (this includes computers and portable storage media (where allowed). Private equipment (i.e. owned by the users) must not be used for the storage of personal data unless otherwise agreed by the school's headteacher. If the headteacher agrees to this then they acknowledge the associated risks and will ensure staff are made aware of these. Staff will also ensure a reasonable level of security is applied to their personal device to minimise the potential for data loss e.g. device lock code or password.

When personal data is stored on any portable computer system, USB stick or any other removable media:

- the data must be encrypted and password protected,
- the device must be password protected
- the device must offer approved virus and malware checking software, and
- the data must be securely deleted from the device

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

The Horizon Multi Academy Trust has clear policy and procedures for the use of "Cloud Based Storage Systems" (for example dropbox, google apps and google docs) and is aware that data held in remote and cloud storage is still required to be protected in line with the Data Protection Act. The school will ensure that it is satisfied with controls put in place by remote / cloud based data services providers to protect the data.

As a Data Controller, the school is responsible for the security of any data passed to a "third party". Data Protection clauses will be included in all contracts where data is likely to be passed to a third party.

All paper based Protected and Restricted (or higher) material must be held in lockable storage, whether on or off site. The Horizon Multi Academy Trust recognises that under Section 7 of the DPA 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 (written request to school's headteacher) 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.

Secure transfer of data and access out of school

The academy 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 restricted or protected personal data from the school or authorised premises without permission from the schools Senior Management Team. The media used must be 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 (eg family members) when out of school
- When restricted or protected 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 have secure remote access to the management information system
- Users must protect all portable and mobile devices, including media, used to store and transmit personal information using approved encryption software; and
- Particular care should be taken if data is taken or transferred to another country, particularly outside Europe, and advice should be obtained to clarify this.

Disposal of data/ Data Retention

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

The disposal of personal 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.

Personal data will be held on ICT systems for a period of 6 months, after this period it will be deleted and no formal backup will be kept. Once an employee leaves the Horizon Multi Academy Trust they'll have a 6 month period from the date of leaving to request copies of any personal information held on personal drives including email. Any request for copies of work will be agreed by the CEO to ensure the business is not jeopardised in anyway by releasing this data.

2.2. Permissive/ non permissive

N/A

2.3. Compliance

Any breaches of school policy may result in criminal, disciplinary or civil action being taken. Action taken will be accordance with the relevant school policies.

3. Key steps in the process

3.1. Roles and responsibilities

The school's headteacher is the Head of IT & Communications. This person 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) in conjunction with the school's SMT

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

what information is held, for how long and for what purpose,
how information as been amended or added to over time, and
who has access to protected data and why.

Everyone in the school has the duty of care 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 to personal data, when engaged in their role as a Governor.

3.2. Procedures

Subject Access Requests

Horizon MAT will respond within 40 days of the original Subject Access request. Any request will be dealt by each school's principal and be checked for authenticity before data is provided. A charge of £10 will also apply.

Freedom of Information Procedures

Freedom of Information requests must be submitted in writing by post or by emailing each school. The headteacher will respond within 20 days of the original request.

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

The school/ academy 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 IRO/SIRO to the Information Commissioner's Office based upon the local incident handling policy and communication plan.

Freedom of Information Policy

All schools are committed to comply with the relevant legislation pertaining to a freedom of information request, and will follow the guidance set out by the Information Commissioner's Office.

3.3. Local conditions statement

In some circumstances, local conditions mean that delivery will require local specific changes in the procedures. However the core essence of the policy must be followed.

Please highlight below any school specific policy changes, this must be signed by the principal of the school and they're responsible for this change in policy guidelines.

School Data Protection Policy

The following staff members are granted full access to the MIS systems within school Personal

data can / cannot be held on personal devices

Appendix 1

Use of Protective Marking

	The information	**The technology**	**Notes on Protect Markings**
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	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 achievement	Individual pupil / student 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.	Via secure systems, 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 Confidential (Level 1) category. There may be students/ pupils whose personal data requires a HIGHLY CONFIDENTIAL marking (Impact Level 2). For example, the home address of a child at risk. In this case, the school may decide not to make this pupil / student 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	Email and text messaging or Learning Platforms or portals might be used to alert parents to issues.	Most of this information will fall into the CONFIDENTIAL (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.

Appendix 2: Privacy Notice Template

PRIVACY NOTICE TEMPLATE
For Pupils in Schools, Alternative Provision and Pupil Referral Units and Children in Early Years Settings

Privacy Notice - Data Protection Act 1998

We, the Horizon Multi Academy Trust, are a data controller for the purposes of the Data Protection Act. We collect information about pupils and may receive information about pupils from their previous school and the Learning Records Service. We hold this personal data and use it to:

Support teaching and learning;
Monitor and report on progress;
Provide appropriate pastoral care, and
Assess how well the school is doing.

This information includes pupil's contact details, national curriculum assessment results, attendance information and personal characteristics such as your ethnic group, any special educational needs and relevant medical information.

We will not give information about pupils to anyone outside the school without parents/carer's consent unless the law and our rules allow us to.

We are required by law to pass some information about pupils to the Department for Education (DfE) and, in turn, this will be available for the use(s) of the Local Authority.

If you want to see a copy of the information about pupils that we hold and/or share, please contact the schools office.

If you require more information about how the DfE store and use information, then please go to the following websites:

http://www.education.gov.uk/researchandstatistics/datatdatam/b00212337/datause

If you are unable to access these websites we can send you a copy of this information. Please contact the DfE as follows: Public Communications Unit, Department for Education
Sanctuary Buildings, Great Smith Street, London
SW1P 3BT
Website: www.education.gov.uk
email: http://www.education.gov.uk/help/contactus
Telephone: 0370 000 2288