Data Protection/GDPR Policy

Policy Adopted 18/01/20

Reviewed 18/01/24

Next review 18/01/2026

Summary

The aim of this policy is to provide a framework to enable staff, parents and pupils to understand:

- the law regarding personal data
- how personal data should be processed, stored, archived and disposed of
- how staff, parents and pupils can access personal data

1. Aims and Objectives

1.1 It is a statutory requirement for all schools to have a Data Protection Policy:

1.2 Data Protection Principles

In accordance with Article 5 of the GDPR, Make it education ltd will ensure that personal data shall be:

a) processed lawfully, fairly and in a transparent manner in relation to individuals;

b) 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, subject to measures respecting the principle of 'data minimisation', not be considered to be incompatible with the initial purposes;

c) adequate, relevant and limited to what is necessary in relation to the purpose for which they are processed;

d) 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;

e) 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 in the public interest, scientific or historical research 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, and again subject to the 'data minimisation' principle; and

f) 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 organisation measures.

Make it education ltd (the controller) shall be responsible for, and be able to demonstrate,

compliance with the principles i.e. its policies and systems comply with requirements of GDPR.

2. Lawful Basis for processing data
The vast majority of information that Make it! will collect and process is required to enable Make it! to perform tasks carried out in the public interest. There are other bases that, such as a specific legal obligation applying to the data controller that makes the processing necessary.

2.1 Age. Children under the age of 13 are not considered able to give consent to process data or to directly access the rights of a data subject, so parents or guardians do this on their behalf. Over the age of 13 this responsibility is transferred to the child and parents will not have responsibility for their child's data.

2.2 Consent. If there is a lawful basis for collecting data then consent to collect data is not required. However, Parents/Carers of children under the age of 13 will need to give consent when there is not a legal reason for processing, for instance for images used in school publicity or social media feeds. The consent will be transparent, revocable, and will be on a "opt-in" basis.

RIGHTS

The GDPR provides for the following rights:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling

For "Privacy notices" covering the right to be informed, please see section 5 below.

Different rights attach to different lawful bases of processing:

Right to erasure, Right to portability, Right to object, Vital Interests ,Legal Obligation ,Public Task ,Legitimate Interests, Consent and right to withdraw consent

The right to erasure. GDPR includes a right to erasure – but this is not an absolute right and does not necessarily override the lawful basis for continuing to hold data. This does not mean the data will never be erased. It will still not be retained for any longer than

necessary, in accordance with statutory
requirements and/or Make it!'s data retention guidelines.

3. Data Types

GDPR defines different types of data and prescribes how it should be treated.

3.1 Personal data

Make it! will have access to a limited range of personal information and data. The data may be held in a digital format or on paper records. Personal data will include:

- Personal information about members of Make it! community – including pupils / students, members of staff and parents / carers e.g. names, addresses, contact details, legal guardianship contact details, disciplinary records
- Curricular / academic data e.g. student progress records, reports, references
- Professional records e.g. employment history, taxation and national insurance records, appraisal records, disciplinary records and references
- Any other information that might be disclosed by parents / carers or by other agencies working with families or staff members.

3.2 Special Category Data

"Special Category Data" is more sensitive, and so needs more protection.

In a school the most likely special category data is likely to be:

- Information on the racial or ethnic origin of a pupil or member of staff
- Information about the sexuality of a child, his or her family or a member of staff
- Medical information about a child or member of staff (SEND)
- Some information regarding safeguarding will also fall into this category

3.3 Other types of Data not covered by the act

This is data that does not identify a living individual and could include Lesson Plans (where no individual pupil is named), Teaching Resources, and other information about Make it! which does not relate to an individual. Some of this data would be available publicly (for instance the diary for the forthcoming year).

4. Responsibilities

The Head of Centre will act as Data Protection Officer

The role of the DPO will include:

- To inform and advise the organisation and its employees about their obligation to comply with the GDPR and other data protection laws

- To monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments; train staff and conduct internal audits
- To be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, customers etc.)

4.2 Risk management – Staff

- Everyone in Make it! has the responsibility of handling personal information in a safe and secure manner

5. Legal Requirements

5.1 Registration

Make it! will be registered as a Data Controller on the Data Protection Register held by the Information Commissioner

5.2 Information for Data Subjects (Parents, Staff): PRIVACY NOTICES

In order to comply with the fair processing requirements of the DPA, Make it! must inform parents / carers of all pupils / students and staff of the data they collect, process and hold on the pupils / students, the purposes for which the data is held, the legal basis for holding it and the third parties (e.g. LA, DfE, etc.) to whom it may be passed. The privacy notice will set out the data subjects' rights under the GDPR. New privacy notices will be issued to all 'data subjects' even if the data subject has previously received a similar
notice.

6. Transporting, Storing and Disposing of personal Data

6.1 Information security – Storage and Access to Data

6.1.1 Technical Requirements

- Make it! 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.
- 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 unattended (even for very short periods).
- 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 (where allowed). Private equipment (i.e. owned by the users) must not be used for the storage of personal data.

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

6.1.2 Portable Devices

When personal data is stored on any portable computer system:

o The data must be encrypted and password protected.
o The device must be password protected.
o The data must be securely deleted from the device, in line with school policy once it has been transferred or its use is complete.
o Data storage of personal information on removal media e.g. USB, portable hard drive, is not allowed, even if encrypted.
o Staff may only use removable media e.g. USB, portable hard drive to transfer non personal information e.g. for use in lesson planning.

Passwords

o All users will use strong passwords which must be changed regularly. User passwords must never be shared.

6.1.3 Images

o Images of pupils (will only be processed and transported by use of authorised agents of the school and permission for this will be obtained in the privacy notice or other photographic permission notice.)
o Images will be protected and stored in a secure area.

6.1.4 Cloud Based Storage

o Make it! has clear policy and procedures for the use of "Cloud Based Storage Systems" and is aware that data held in remote and cloud storage is still required to be protected in line with the Data Protection Act. Make it! will ensure that it is satisfied with controlsput in place by remote / cloud based data services providers to protect the data.

6.2 Third Party data transfers

As a Data Controller, the academy is responsibility for the security of any data passed to a "third party". Data Protections clauses will be included in all contracts where data is likely to be passed to a third party as well as data processing agreements.

6.3 Retention of Data

o The guidelines given by the Information and Records Management Society – Schools records management toolkit will be used to determine how long data is retained.
o Personal data that is no longer required will be destroyed and this process will be recorded.

6.4 Systems to protect data

6.4.1 Paper Based Systems

○ All paper based personal data will be protected by appropriate controls, for example:
♣ Paper based safeguarding chronologies will be in a locked cupboard when not in use
♣ Class lists used for the purposes of marking may be stored in a teacher's bag
○ Paper based personal information sent to parents will be checked before the envelope is sealed.

6.4.2 School Websites

○ Uploads to Make it! website will be checked prior to publication, for instance:
♣ To check that appropriate photographic consent has been obtained
♣ To check that the correct documents have been uploaded

6.4.3 E-mail

○ Where technically possible all e-mail containing sensitive information must be encrypted.
○ The use of a secure e-mail system allows for secure communication.

7. Data Sharing

Make it! is required by law to share information with the LA and DfE.

8. Data Breach – Procedures

In the event of a data breach the data protection officer will inform partner schools.

9. Policy Review Reviewing:

This policy will be reviewed, and updated if necessary every two years or when legislation changes.