

GDPR Policy: School Workforce Acceptable use of ICT Policy 23/24



Document Control

A. Confidentiality Notice	This policy document has been approved by the Governing Body of St Modwen's Catholic Primary School and is intended for internal and/or external publication. Where the document is identified for internal use the policy information may not be shared with external agencies or parents without the prior agreement of the Headteacher or authorizing committee.																			
B. Document Details	Classification:		Premises, Health and Safety Committee																	
	Policy Source:		John Walker (Data Protection Officer) May 2023 Version																	
	Organisation:		St Modwen's Catholic Primary School																	
	Documents reference:		Policy number: STM50																	
	Current Version Number:		V1(5 pages)																	
	Current Document Approved by: (Committee)		PH & S																	
	Date Approved:		Autumn 2 Term 2023																	
	Statutory Policy		Yes																	
	Internal/External Policy (published on website)		External – Publish on website																	
	Schedule Review:		Next Review date:		Review cycle															
Autumn Term 2 2024			Annually																	
C. Version Control Document revision and Approval History	<table border="1"> <thead> <tr> <th data-bbox="528 1503 652 1615">Version</th> <th data-bbox="652 1503 794 1615">Date</th> <th data-bbox="794 1503 954 1615">Version created by:</th> <th data-bbox="954 1503 1114 1615">Version approved by:</th> <th data-bbox="1114 1503 1489 1615">Comments</th> </tr> </thead> <tbody> <tr> <td data-bbox="528 1615 652 1850">V1</td> <td data-bbox="652 1615 794 1850">7.11.2023</td> <td data-bbox="794 1615 954 1850">School</td> <td data-bbox="954 1615 1114 1850">PH & S</td> <td data-bbox="1114 1615 1489 1850">Revised August 2023 – John Walker Policy 13.5.2023 refresh Amends: 2 Data Portability p2 added 2018 4 GDPR related policies – updated new GDPR policies</td> </tr> <tr> <td data-bbox="528 1850 652 1879"></td> <td data-bbox="652 1850 794 1879"></td> <td data-bbox="794 1850 954 1879"></td> <td data-bbox="954 1850 1114 1879"></td> <td data-bbox="1114 1850 1489 1879"></td> </tr> </tbody> </table>					Version	Date	Version created by:	Version approved by:	Comments	V1	7.11.2023	School	PH & S	Revised August 2023 – John Walker Policy 13.5.2023 refresh Amends: 2 Data Portability p2 added 2018 4 GDPR related policies – updated new GDPR policies					
	Version	Date	Version created by:	Version approved by:	Comments															
V1	7.11.2023	School	PH & S	Revised August 2023 – John Walker Policy 13.5.2023 refresh Amends: 2 Data Portability p2 added 2018 4 GDPR related policies – updated new GDPR policies																

D. Contents	Section	Page No
	1. School Policy	2
	2. Data Portability	2
	3. Acceptable use policy agreements	3-4
	4. GDPR related policies	5

School Workforce Acceptable use of ICT Policy 23/24

1. School policy

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe internet access at all times.

2. Data Portability

The UK GDPR requires an organisation that stores data to enable transfer of that data from one organisation to another. In schools, pupil data is transferred using the Common Transfer File (CTF) which is a DfE standard process. This is outside the scope of data portability in the UK GDPR.

Employee data will be shared to enable new starters and leavers to take up new roles as easily as possible.

When new data is provided to school it will then be administered and processed within the terms of the Data Protection 2018 and any other relevant policy

THIS ACCEPTABLE USE POLICY IS INTENDED TO ENSURE THAT

- staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- staff are protected from potential risk in their use of ICT in their everyday work.
- school complies with guidance set out in GDPR (2018)

The school will try to ensure that staff and volunteers will have good access to ICT to enhance their work, to enhance learning opportunities for students / pupils learning and will, in return, expect staff and volunteers to agree to be responsible users.

This policy supports school:

- Safeguarding Policy – reference Appendix 1 – List of school related safeguarding policies
- 9. GDPR related policies for compliance

3. Acceptable use policy agreement

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that students / pupils receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed e-safety in my work with young people.

FOR MY PROFESSIONAL AND PERSONAL SAFETY:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of school ICT systems (eg laptops, email, VLE etc) out of school.
- I understand that the school ICT systems are primarily intended for educational use.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person (Information Security Officer/Head Teacher).
- I understand and accept my obligations under GDPR (2018)

I WILL BE PROFESSIONAL IN MY COMMUNICATIONS AND ACTIONS WHEN USING SCHOOL ICT SYSTEMS:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (eg on the school website / VLE) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use chat and social networking sites in school in accordance with the school's policies and particular using twitter:
 - I will not use the St.Modwen's Catholic Primary School logo for my feed. This is reserved for the official St.Modwen's Catholic Primary School feed only. I will set up an account carefully and will closely monitor my 'bio'.
 - I will not follow students back on their twitter/social media accounts
 - I will avoid entering into conversations with students using twitter/social media accounts, especially any feeds I set up under the St.Modwen's Catholic Primary School banner i.e. department or team.
 - I will be careful uploading photographs of students and I will not associate names with any faces.
 - I will not use students @ names in tweets because this makes the student 'followable' by anyone.
- I will only communicate with students/pupils and parents/carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.
- The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:
- I will not store personal/sensitive data on personal USB's/unencrypted devices/personal laptops/mobile phones. I accept that if I need to access personal/sensitive data held by the school outside of the school environment I will use remote access 'athome' or if this is not feasible use an encrypted USB stick supplied by school.
- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.
- I will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.

- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School Data Protection/Data Sharing policy where personal data is transferred outside the secure school network, it must be encrypted.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I understand that data protection policy requires that any staff or student / pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

WHEN USING THE INTERNET IN MY PROFESSIONAL CAPACITY OR FOR SCHOOL SANCTIONED PERSONAL USE:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I UNDERSTAND THAT I AM RESPONSIBLE FOR MY ACTIONS IN AND OUT OF SCHOOL:

- I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment out of school and my use of personal equipment in school or in situations related to my employment by the school.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and / or the Local Authority, referral to the ICO in the case of a serious breach and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff/Volunteer/Governor Name	
Signature:	
Date:	

4. GDPR Related Policies

	Review Date
01 Data Protection Policy	September 2024
02 Breach and Non-Compliance Policy	September 2024
03 Confidentiality Policy and Confidential Agreements	September 2024
04 CCTV Policy	September 2024
05 Workforce Acceptable use Policy	September 2024
06 Freedom of Information Policy	September 2024
07 Document and Data Retention Policy	September 2024
08 Privacy Notices: <ul style="list-style-type: none"> • Pupils Data • School Trips • Staff Workforce • Governors • Job Applicants • PTA • External School Photographer 	September 2024
09 GDPR Workforce and Governor Training/CPD <ul style="list-style-type: none"> • GDPR Guidelines for staff 	September 2024
10 GDPR Checks, Compliance and Audit Toolkit (GoGDPR)	September 2024
11 GDPR Subject Access Request Management and Procedures	September 2024
12 GDPR My rights a guide for data subjects	September 2024
13 GDPR Home School Communication Charter	September 2024
14 GDPR Information Security Protocol	September 2024
15 Cyber Response Plan	September 2024