

D1.2

Data Management Plan and Ethics Guidelines

Version 1.0

Work package	Project management and coordination
Task	T1.3 - T1.4
Due date	30-04-2026
Submission date	08-05-2026
Deliverable lead	V. N. Karazin Kharkiv National University (KKNU)
Version	V1.0
Authors	Iryna Shteimiller (KKNU)
Reviewers	Svitlana Zhytsova (DONNU), Nataliia Kriuchkova (ONU), Magda Spella (HOU)

Abstract

This document constitutes Deliverable D1.2 - Data Management Plan and Ethics Guidelines of the Erasmus+ Capacity Building in Higher Education project “BOOSTSCIENCE - Boosting Education Quality and Entrepreneurial Mindsets for Natural Sciences in Ukraine”. It establishes the consortium-wide procedures for the collection, processing, monitoring, classification, storage, sharing, preservation and dissemination of project data throughout the project lifetime. It also defines ethics and gender management guidelines, informed consent procedures, personal data protection safeguards, and practical templates to be used when human participants are involved in surveys, interviews, evaluations, learning analytics, dissemination activities or other project-related data collection.

The DMP and Ethics Guidelines operationalise the data management and ethics management principles set out in the Project Management Plan and align them with the requirements of the Grant Agreement, Consortium Agreement, Erasmus+ rules, EU data protection principles and relevant national and institutional policies. The document is designed as a living instrument and may be updated during the project when data categories, tools, processing purposes, risks or ethical requirements change.

Keywords

Data Management Plan; Ethics Guidelines; GDPR; informed consent; gender mainstreaming; personal data protection; FAIR data

Document revision history

Version	Date	Description of change	Contributor(s)
v0.1	28.04.2026	First draft for internal review	Iryna Shteimiller (KKNU)
v0.2	30.04.2026	Reviewed by the partners	Svitlana Zhyltsova (DONNU), Nataliia Kriuchkova (ONU), Magda Spella (HOU)
v0.3	04.05.2026	Updated version	Iryna Shteimiller (KKNU)
v1.0	08.05.2026	Final version	Magda Spella (HOU) Kyriakos Bourikas (HOU)

Disclaimer

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

The information available in this deliverable is provided by the BOOSTSCIENCE consortium under EC grant agreement **101237769**.

Nature of the deliverable

DMP

Dissemination level

PU Public

SEN Sensitive



* Deliverable types:

[R — Document, report]
[DEM — Demonstrator, pilot, prototype]
[DEC — Websites, patent filings, videos, etc]
[DATA — data sets, microdata, etc]
[DMP — Data Management Plan]
[ETHICS]
[SECURITY]
[OTHER]

Table of contents

Executive summary	7
1 Introduction	8
1.1 Overview of BOOSTSCIENCE project	8
1.2 Purpose and scope of D1.2	9
1.3 Relationship with project management and quality assurance	9
1.4 Guiding principles	9
2 Data governance and responsibilities	10
2.1 Governance structure for data and ethics	10
2.2 Roles and responsibilities	10
2.3 Review cycle and escalation	10
3 Data inventory and lifecycle.....	11
3.1 Expected data categories.....	11
3.2 Data classification	12
3.3 Data lifecycle.....	12
3.4 Data minimisation rules.....	13
4 FAIR data management and dissemination.....	13
4.1 FAIR approach.....	13
4.2 File formats and naming	13
4.3 Open access, licensing and IPR	13
5 Personal data protection, security and retention.....	14
5.1 Data protection principles	14
5.2 Lawful basis and consent.....	14
5.3 Informed consent and privacy notices	14
5.4 Security and access control.....	14
5.5 Data breach and incident response	15
5.6 Retention and deletion	15
6 Ethics and gender guidelines.....	16
6.1 Core ethics principles.....	16
6.2 Human participants in surveys and evaluation	16
6.3 Students, power relations and voluntariness	16
6.4 Gender equality, inclusion and non-discrimination	16
6.5 Conflict-sensitive implementation in Ukraine.....	17
6.6 Academic integrity, IPR and responsible digital practice	17
6.7 Health, safety and environmental considerations	17
7 Operational procedures	18
7.1 Ethics and data protection screening before data collection	18
7.2 Retention and deletion standard survey procedure	18
7.3 Publication and dissemination procedure.....	18
7.4 Data transfer between partners	18
7.5 Monitoring and reporting.....	18
8 Monitoring, updates and conclusions.....	19

Annex 1. Data inventory template	20
Annex 2. Participant information sheet and consent form template	21
Annex 3. Short privacy notice template for online surveys	22
Annex 4. Ethics and gender screening checklist	23
Annex 5. Data incident reporting form.....	24
Annex 6. VLE and learning analytics register	25

List of tables

Table 1. BOOSTSCIENCE consortium	9
Table 2. Roles and responsibilities for DMP and ethics in BOOSTSCIENCE.....	10
Table 3. BOOSTSCIENCE initial data inventory	12
Table 4. Data classification.....	12
Table 5. BOOSTSCIENCE approach to make data FAIR	13
Table 6. BOOSTSCIENCE retention approach	15

Abbreviations

CA	Consortium Agreement
DMP	Data Management Plan
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer or responsible institutional data protection contact
EACEA	European Education and Culture Executive Agency
EC	European Commission
FAIR	Findable, Accessible, Interoperable and Reusable
GA	Grant Agreement
GDPR	General Data Protection Regulation (Regulation (EU) 2016/679)
HEI	Higher Education Institution
IPR	Intellectual Property Rights
PC	Project Coordinator
PMT	Project Management Team
SC	Steering Committee
VLE	Virtual Learning Environment
WP	Work Package

Executive summary

D1.2 provides the operational framework for data management and ethics in BOOSTSCIENCE. The project produces management, educational, evaluation, dissemination and stakeholder engagement data. It may also collect personal data from project staff, academic staff, students, labour market stakeholders and event participants through surveys, interviews, registration forms, attendance lists, feedback forms and the Virtual Learning Environment. The plan defines how those data will be handled in a transparent, secure, proportionate and legally compliant manner.

The central principle of this DMP is privacy-by-design and ethics-by-design. Project partners will only collect data that are necessary for project purposes; will inform participants clearly about how data will be used; will apply informed consent procedures where participation in surveys, interviews or evaluation activities is requested; and will anonymise or aggregate results before dissemination whenever identification is not required.

The Ethics Guidelines complement the DMP by defining practical safeguards for voluntary participation, gender equality and non-discrimination, academic integrity, responsible use of digital tools and learning analytics, intellectual property, and conflict-sensitive implementation in the Ukrainian context. All partners are responsible for applying these procedures in their institutional activities, while KGNU leads D1.2 implementation in coordination with HOU, the PMT, WP leaders and the Steering Committee.

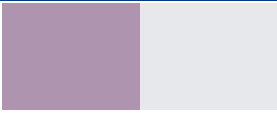
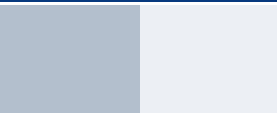
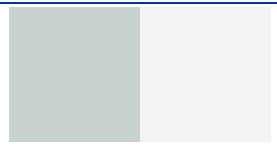
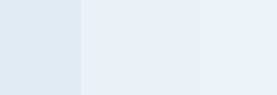
1 Introduction

1.1 Overview of BOOSTSCIENCE project

“BOOSTSCIENCE - Boosting Education Quality and Entrepreneurial Mindsets for Natural Sciences in Ukraine - is an Erasmus+ Capacity Building in Higher Education project under Grant Agreement No. 101237769. The project responds to the urgent need to modernise Biology and Chemistry education in Ukraine, strengthen university-industry links, and equip master-level students with research, entrepreneurial and labour-market-oriented competences.

The project develops an interdisciplinary master-level module supported by digital and virtual learning approaches, including remote laboratories, research-based activities, work-based and problem-based activities, entrepreneurial learning, capacity building for Ukrainian HEIs, and dissemination and sustainability activities. The project runs for 36 months and involves 12 partners from Greece, Spain and Ukraine.

BOOSTSCIENCE is comprised of 12 partners and is coordinated by Hellenic Open University (HOU, Greece), as shown in **Table 1** below:

Number	Short name	Legal name	Country	Logo
1	HOU	Hellenic Open University	Greece	
2	KKNU	V.N. Karazin Kharkiv National University	Ukraine	
3	UJI	Universitat Jaume I de Castellón	Spain	
4	Uoi	University of Ioannina	Greece	
5	LNS	Leanspots	Spain	
6	DONNU	Vasyl' Stus Donetsk National University	Ukraine	
7	CNU	Vasyl Stefanyk Carpathian National University	Ukraine	
8	IFNUL	Ivan Franko National University of Lviv	Ukraine	
9	ONU	Odesa I.I. Mechnikov National University	Ukraine	

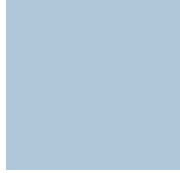
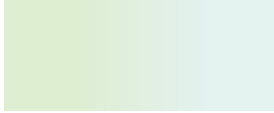
10	SSI ISC	State Scientific Institution "Institute for Single Crystals" of National Academy of Sciences of Ukraine	Ukraine	
11	BIOTEK	Pharmaceutical company "FK"Biotech Ltd."	Ukraine	
12	UORSY	Limited Liability Company «Research and Production Enterprise «Ukrorgsyntez», Ukrorgsyntez LTD	Ukraine	

Table 1. BOOSTSCIENCE consortium

1.2 Purpose and scope of D1.2

D1.2 covers the procedures that apply to project data and ethical conduct across all work packages. It specifies how data will be collected, processed, monitored, classified, stored, shared, archived and disseminated during the project lifetime. It also sets out informed consent procedures for human participation in surveys, interviews, feedback activities and data processing connected to project implementation.

The scope covers both personal and non-personal data, including administrative records, deliverables, stakeholder consultation data, educational materials, Virtual Learning Environment data, evaluation results, attendance lists, communication metrics, photos and recordings where applicable, and aggregated project indicators. It does not replace institutional data protection policies; where institutional or national rules are stricter, the stricter standard applies.

1.3 Relationship with project management and quality assurance

The Project Management Plan identifies data management and ethics management as specific consortium procedures. D1.2 operationalises these procedures by translating them into concrete rules, responsibilities, templates and checklists. D1.3 Quality Assurance Plan will complement this document by defining quality indicators, monitoring and risk management instruments. The DMP will therefore function together with the PMP, QAP, Consortium Agreement, Grant Agreement and WP-specific implementation plans.

1.4 Guiding principles

- ☐ Purpose limitation: data will be collected only for clearly defined BOOSTSCIENCE purposes.
- ☐ Data minimisation: only data necessary for project implementation, reporting, evaluation and dissemination will be collected.
- ☐ Transparency: participants will receive clear information before data collection.
- ☐ Security and confidentiality: access will be limited to authorised project staff and protected through appropriate technical and organisational measures.
- ☐ FAIR and open science where possible: non-sensitive outputs will be made findable, accessible, interoperable and reusable whenever this is compatible with privacy, IPR and grant rules.
- ☐ Ethics-by-design: ethical risks will be assessed before data collection and monitored throughout implementation.
- ☐ Gender equality and inclusion: activities will avoid discrimination and will seek balanced participation where feasible.

2 Data governance and responsibilities

2.1 Governance structure for data and ethics

Data and ethics governance follows the general BOOSTSCIENCE governance model. The Steering Committee provides strategic oversight and resolves issues that cannot be solved at operational level. The Project Coordinator, HOU, ensures alignment with the Grant Agreement and communication with EACEA. KGNU, as D1.2 lead and Ukrainian coordination support point, coordinates the implementation of data management and ethics procedures across Ukrainian partners. The Project Management Team and WP leaders ensure that data and ethics requirements are embedded in WP activities.

Each partner is responsible for lawful and ethical processing of data under its control, maintaining records of data collection activities, securing institutional files, and ensuring that staff involved in data processing understand this DMP. Partners should identify an internal contact person for data protection and ethics matters and should consult their institutional DPO or legal/data protection office where applicable.

2.2 Roles and responsibilities

Role/body	Main responsibilities for DMP and ethics
Steering Committee	Approves major changes to data and ethics procedures; resolves escalated issues; ensures consortium-wide compliance.
Project Coordinator - HOU	Ensures consistency with GA/CA and project reporting; coordinates with EACEA where necessary; monitors implementation through PMT and reporting workflows.
D1.2 Lead - KGNU	Maintains this DMP; coordinates data and ethics templates; supports Ukrainian HEIs; consolidates updates and issues for PMT/SC review.
Project Management Team	Embeds DMP and ethics requirements in WP delivery; reviews data risks; coordinates mitigation actions.
WP Leaders	Ensure that WP tasks use approved tools, consent forms, privacy notices and secure storage; report changes in data collection or ethics risks.
All partners	Collect only necessary data; inform participants; protect files; respect retention rules; notify incidents; follow local institutional requirements.
Institutional DPO/data protection contact	Provides advice on GDPR, national data protection law, DPIA needs and breach handling where relevant.

Table 2. Roles and responsibilities for DMP and ethics in BOOSTSCIENCE

2.3 Review cycle and escalation

D1.2 is a living document. It should be reviewed at least at mid-term, before the final reporting period, and whenever a new tool, data category, data transfer, data processor, evaluation method, or ethical risk is introduced. Minor clarifications may be introduced by the D1.2 lead in coordination with the PC. Material changes that affect partners' rights, participant rights, security risks or dissemination of personal/sensitive information should be submitted to the PMT and, where necessary, to the SC.

Any data protection or ethics concern should first be reported to the WP leader and D1.2 lead. Urgent incidents, suspected breaches, complaints from participants, or risks that may affect the project should be reported immediately to the PC and escalated to the PMT/SC according to the project management procedure.

3 Data inventory and lifecycle

3.1 Expected data categories

BOOSTSCIENCE will generate and process several categories of data. **Table 3** below provides an initial data inventory. WP leaders will update the inventory when specific surveys, evaluation tools, VLE functions, dissemination actions or reporting instruments are finalised.

Dataset / source	Main data elements	Classification	Storage, sharing and retention
Project management records	Partner contact lists, meeting agendas, minutes, decisions, attendance sheets, internal reports, financial reporting summaries	Internal; may contain professional contact data	Stored in Basecamp/project folders and institutional systems. Shared with consortium and EACEA where required. Retained according to GA/audit obligations.
Needs assessment and stakeholder consultation	Survey/interview responses from students, academics and labour market actors; aggregated skill-gap results; institutional context data	Personal data possible; sensitive data not intended	Collect through approved tools. Analyse in pseudonymised/anonymised form. Public dissemination only in aggregate.
Curriculum and educational materials	Syllabi, presentations, documents, quizzes, videos, remote lab instructions, VLE resources, Ukrainian auxiliary content	Mostly non-personal; copyright/IPR-relevant	Stored in VLE/project repositories. Disseminated publicly where cleared for rights and licensing.
VLE and learning analytics	User registration, enrolment, access logs, quiz results, completion status, grades or progress indicators	Personal data; confidential educational records	Access limited to authorised teaching/evaluation staff. Export only pseudonymised or aggregated data for project evaluation.
Pilot module evaluation	Student/staff feedback, observations, completion rates, grades, module satisfaction, recommendations for improvement	Personal data possible; research/evaluation data	Use informed consent or institutional evaluation basis as appropriate. Disseminate aggregate findings only.
Capacity building and study visits	Registration data, attendance, feedback questionnaires, photos/videos where consented, travel/participation records	Personal data; possible image data	Use registration privacy notices and photo/recording consent or opt-out procedures. Retain as needed for reporting/audit.
Dissemination and visibility	Website/news items, social media metrics, event lists, publications, stakeholder contacts, visual materials	Public or internal; image/contact data possible	Publish only approved content. Avoid exposing personal data without consent or legitimate project purpose.

Quality assurance and monitoring	KPI data, internal/external evaluation results, risk logs, corrective actions, partner feedback	Internal; may include personal opinions	Shared within PMT/SC. Public reports use anonymised/aggregated findings.
----------------------------------	---	---	--

Table 3. BOOSTSCIENCE initial data inventory

3.2 Data classification

All project data should be classified before storage and sharing (Table 4). The following classification is used:

Class	Description	Examples	Default access
Public	Information approved for external dissemination.	Public deliverables, open educational materials, project news.	Public website, repositories, VLE open area.
Internal	Project working information not intended for public release.	Drafts, internal minutes, contact lists, internal reports.	Consortium members with need-to-know access.
Confidential	Information that could affect individuals, institutions or project interests if disclosed.	Raw survey data, financial details, evaluation comments, non-public partner information.	Restricted authorised staff only.
Sensitive / special case	Data requiring enhanced safeguards or prior approval.	Special category personal data, security-relevant information, identifiable vulnerable participant information.	Avoid collection unless strictly necessary; consult DPO/PC/SC before processing.

Table 4. Data classification

3.3 Data lifecycle

The data lifecycle applies to each dataset from planning to deletion or archiving. WP leaders must ensure that the lifecycle steps are documented before data collection starts.

- Plan: define purpose, data owner, participants, tool, lawful basis/consent, retention period and dissemination plan.
- Collect: use approved templates, collect only necessary fields, inform participants and obtain consent where required.
- Store: save data in secure institutional or project systems; restrict access; avoid local copies where not necessary.
- Process and analyse: use pseudonymised data where possible; keep identifiers separate from responses; document transformations.
- Share: share personal or confidential data only with authorised partners and only for agreed project purposes.
- Disseminate: publish only anonymised, aggregated or rights-cleared outputs.
- Archive or delete: retain data for the period required for project reporting/audit and delete/anonymise data when no longer necessary.

3.4 Data minimisation rules

Project partners should avoid collecting national identification numbers, private addresses, exact geolocation, political opinions, health data, sensitive war-related personal experiences, biometric data, or any special category data unless a specific, documented and approved purpose exists. Surveys should allow non-response to demographic questions. Gender-disaggregated monitoring may be useful for equality analysis, but gender data should be optional and reported only in aggregate.

4 FAIR data management and dissemination

4.1 FAIR approach

The project will apply the FAIR principles to non-sensitive outputs and data where feasible (Table 5). FAIR implementation must not compromise personal data protection, confidentiality, security, IPR or legitimate project interests. The default approach is open access for public deliverables, educational materials and aggregated findings, while raw personal data and confidential internal data remain restricted.

FAIR principle	BOOSTSCIENCE implementation
Findable	Public deliverables and educational outputs will use clear titles, authors, dates, version numbers, keywords, project acronym, grant number and WP references.
Accessible	Public outputs will be made available through the project website, VLE/open area and/or institutional repositories where appropriate. Restricted datasets will have documented access conditions.
Interoperable	Common and open formats will be preferred, including DOCX/PDF for documents, XLSX/CSV for tables, MP4 for videos, PNG/JPEG for images, and standard survey export formats.
Reusable	Educational materials and aggregated datasets will include licensing, authorship and reuse conditions. Third-party materials will be reused only where permission/licence allows.

Table 5. BOOSTSCIENCE approach to make data FAIR

4.2 File formats and naming

Files should follow a consistent naming convention: BOOSTSCIENCE_WP_Deliverable-or-Activity_Title_Version_Date. Example: BOOSTSCIENCE_D1.2_DMP_Ethics_v1.0_2026-04-30. Version control should distinguish drafts, reviewed versions and final submitted versions. File names should not include personal data unless strictly necessary.

Recommended formats are: DOCX for editable reports, PDF for public final versions, XLSX/CSV for structured data, PPTX/PDF for presentations, MP4 for video, PNG/JPEG for images, MP3/WAV for audio where consented, and ZIP only when multiple related files must be transferred. Password-protected archives should be used for confidential transfer only when no better secure platform is available.

4.3 Open access, licensing and IPR

Public deliverables and educational materials should be disseminated in accordance with the GA, Consortium Agreement and project communication plan. Open licensing, such as Creative Commons Attribution (CC BY 4.0), should be considered for educational materials unless restricted by third-party rights, institutional policies, partner agreements, confidentiality or security considerations.

Before publication, each WP leader must verify that: authors and contributors are acknowledged; no personal data are disclosed without a valid basis; third-party images, datasets, videos, texts and software are used lawfully; and confidential partner information has been removed or approved for publication.

5 Personal data protection, security and retention

5.1 Data protection principles

All partners must process personal data in accordance with applicable EU, national and institutional data protection rules. For EU partners, the GDPR applies directly. For Ukrainian partners, national personal data protection law and institutional policies apply, while GDPR-level safeguards should be followed for project consistency and for data exchanged with EU partners.

The following principles apply across BOOSTSCIENCE: lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity and confidentiality; and accountability. Partners must be able to demonstrate how these principles are applied in their activities.

5.2 Lawful basis and consent

The project may use different lawful bases depending on the activity and institutional context, such as performance of grant-related tasks, legitimate interest in project evaluation and reporting, public interest/educational tasks of HEIs, or informed consent. Consent is required or strongly recommended for surveys, interviews, optional feedback forms, photos/videos, recordings and any data processing that goes beyond ordinary project administration.

Consent must be freely given, specific, informed and unambiguous. Participants must be told that they may refuse to participate or withdraw from optional data collection without negative consequences. Consent forms should be stored separately from survey/interview responses where possible.

5.3 Informed consent and privacy notices

Before collecting personal data from individuals, partners must provide a concise privacy notice explaining: the project identity; data controller/contact point; purpose of processing; categories of data; whether participation is voluntary; who will access the data; how long data will be kept; whether data will be transferred to other partners/countries/tools; participant rights; and whom to contact with questions or complaints.

For online surveys, the information notice and consent statement should appear before the first question. For interviews or recordings, consent should be documented in writing or through an auditable electronic procedure. For events, participants should receive a registration privacy notice and clear information about photography/recording zones or opt-out procedures.

5.4 Security and access control

Project data must be stored in approved project or institutional systems. The Project Management Plan identifies Basecamp as a project management and file storage environment for internal collaboration. Access should be role-based and limited to people who need the data for project tasks. Partners should avoid sharing

raw personal data by email; where email transfer is unavoidable, encrypted or password-protected files should be used and passwords should be sent separately.

- ❑ Use institutional accounts and strong passwords; enable multi-factor authentication where available.
- ❑ Restrict folders containing raw survey data, consent forms, attendance lists, financial documents and VLE exports.
- ❑ Keep consent forms and identifiers separate from response datasets.
- ❑ Remove personal identifiers before analysis and public reporting wherever possible.
- ❑ Avoid storing project data on personal devices unless necessary; if used, devices must be protected and backed up.
- ❑ Delete duplicate or obsolete local copies once data have been transferred to the approved storage location.

5.5 Data breach and incident response

A data incident includes any accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal or confidential project data. Examples include lost devices, misdirected email attachments, unauthorised folder sharing, malware, publication of identifiable survey responses, or unauthorised access to VLE data.

Any suspected incident must be reported immediately to the WP leader, D1.2 lead and PC. The responsible partner should preserve evidence, limit further exposure, assess the affected data and individuals, consult the institutional DPO/data protection contact, and follow institutional/national notification obligations. The PMT and SC should be informed where the incident may affect project implementation or external reporting.

5.6 Retention and deletion

Data should not be kept longer than necessary. Administrative, financial and evidence files required for EACEA reporting, audit and verification should be retained according to GA/CA and institutional rules. Raw personal data from surveys, interviews and evaluations should be anonymised or deleted after analysis and reporting unless there is a documented need to retain them for verification. Public deliverables and educational materials may be preserved longer for sustainability and reuse. The retention and deletion policy is summarised in **Table 6**.

Data type	Suggested retention approach
Grant administration, deliverables, financial and audit evidence	Retain according to GA/CA, audit and institutional retention obligations.
Raw survey/interview data	Retain until analysis/reporting are complete, then anonymise or delete where feasible.
Consent forms	Retain separately for the period needed to demonstrate valid consent, then delete securely.
VLE learning records	Retain according to educational/institutional rules; export for project reporting only in aggregated/pseudonymised form.
Public educational materials and reports	Preserve for sustainability and reuse where IPR and licensing allow.
Photos/videos/recordings	Retain only for the stated communication/training purpose and review periodically.

Table 6. BOOSTSCIENCE retention approach

6 Ethics and gender guidelines

6.1 Core ethics principles

BOOSTSCIENCE is an educational capacity-building project and does not plan clinical research, medical interventions, human biological sample collection, genetic testing of participants, animal experiments or security-sensitive research. If any partner proposes an activity that would introduce such elements, the activity must not start until the ethical, legal, institutional and grant-related implications have been reviewed and approved.

- ❑ Respect for persons: participation in surveys, interviews and feedback activities must be voluntary and informed.
- ❑ Beneficence and non-maleficence: activities should maximise educational and societal benefit while minimising burden and risk to participants.
- ❑ Justice and inclusion: access to activities should be fair, non-discriminatory and sensitive to barriers faced by participants in Ukraine.
- ❑ Confidentiality: information provided by participants must be protected and reported in a way that avoids unwanted identification.
- ❑ Integrity: project outputs must be accurate, evidence-based, properly attributed and free from plagiarism or manipulation.

6.2 Human participants in surveys and evaluation

Human participation is expected mainly through needs assessment, stakeholder consultations, training/event feedback and evaluation of the pilot module. These activities are low-risk when properly designed. Each activity involving human participants must have a clear purpose, responsible partner, target group, data fields, consent/privacy information, data storage location, analysis plan and dissemination plan.

Surveys should avoid unnecessary sensitive questions and should allow participants to skip optional demographic fields. Interviews should use semi-structured guides approved by the WP leader. Recordings should not be made by default; if recording is necessary, explicit consent must be obtained and participants must be able to participate without being recorded where feasible.

6.3 Students, power relations and voluntariness

Because BOOSTSCIENCE activities involve students, special care is required to avoid real or perceived pressure. Participation in optional project surveys, interviews, photos, testimonials or dissemination activities must not affect grades, access to learning opportunities, relationships with teachers, or institutional services. When feedback is collected by a teacher, students should be informed that refusal or critical comments will not have negative consequences. Anonymous or pseudonymous feedback channels should be preferred where feasible.

Learning analytics and grades may be necessary for educational management and evaluation; however, project reporting should use aggregated or pseudonymised data. Individual student performance must not be published or shared outside the authorised educational/evaluation team.

6.4 Gender equality, inclusion and non-discrimination

BOOSTSCIENCE will mainstream gender equality and inclusion across project activities. This includes balanced representation in events and consultations where feasible, inclusive language in materials, accessible

online/hybrid participation options, and attention to barriers caused by displacement, caregiving responsibilities, disability, mobility restrictions, energy insecurity or limited internet access.

Gender-related data may be collected for monitoring only when relevant, optional and proportionate. Reports should present gender-disaggregated findings only in aggregated form and should avoid conclusions based on very small groups that could identify individuals. The project will not tolerate discrimination, harassment or exclusion based on gender, age, disability, ethnic or national background, language, religion, social status or other protected characteristics.

6.5 Conflict-sensitive implementation in Ukraine

The Ukrainian context requires additional sensitivity. Project activities should avoid collecting information that could endanger participants, institutions or communities, such as exact locations of individuals during security-sensitive periods, military-related information, political opinions, details of trauma, or security vulnerabilities. Participation must remain low-burden and flexible, recognising disruptions caused by war, relocation, electricity blackouts, restricted mobility and psychological stress.

When public dissemination includes Ukrainian participants or institutions, partners should check whether names, locations, photos or details could create security or reputational risks. The safest approach is to publish aggregated results and use explicit consent for identifiable images, quotes and testimonials.

6.6 Academic integrity, IPR and responsible digital practice

All project outputs must respect academic integrity and IPR. Educational materials must properly cite sources, avoid plagiarism, respect third-party licences and distinguish original project content from adapted resources. Partners should use plagiarism checks or internal review where appropriate. Where AI-assisted tools are used to support drafting, translation, editing or learning content preparation, human experts remain responsible for accuracy, bias control, confidentiality and final approval.

Confidential project or personal data should not be uploaded to external AI tools unless the institutional rules and tool terms clearly permit such processing and appropriate safeguards are in place. AI-generated or AI-assisted outputs must be reviewed for factual accuracy, copyright issues, bias, accessibility and suitability for Ukrainian HEI contexts.

6.7 Health, safety and environmental considerations

BOOSTSCIENCE uses virtual and remote learning environments to support practical training where physical placements or laboratory access may be difficult. Virtual laboratories and simulations should clearly distinguish simulated procedures from real laboratory practice. When materials refer to chemical, biological or pharmaceutical procedures, they should include appropriate safety disclaimers and must not encourage unsupervised real-life experimentation outside institutional safety protocols.

No project activity should require students to handle hazardous substances, biological materials or laboratory equipment without institutional supervision, safety training and compliance with local safety rules. Environmental sustainability should be considered when organising mobility, events, equipment use, printing and digital storage.

7 Operational procedures

7.1 Ethics and data protection screening before data collection

Before launching a survey, interview, feedback form, VLE data export, photo/video collection or stakeholder consultation, the responsible partner should complete a short screening using Annex 4. The screening should be reviewed by the WP leader and, where needed, by the D1.2 lead or institutional DPO/data protection contact.

Activities that involve only anonymous aggregate data or standard event registration may proceed after WP-level review. Activities that involve identifiable vulnerable participants, sensitive data, recordings, cross-border transfer of raw personal data, external processors with unclear terms, or publication of identifiable quotes/images should be escalated to the D1.2 lead and PC before launch.

7.2 Retention and deletion standard survey procedure

- ☐ Define the purpose, target group, required indicators and dissemination plan.
- ☐ Prepare the questionnaire using minimal data fields and neutral wording.
- ☐ Add the privacy notice and consent statement at the start of the survey.
- ☐ Use institutional or approved survey tools and restrict access to exports.
- ☐ Export and analyse data in pseudonymised/anonymised form where possible.
- ☐ Publish only aggregated results and remove free-text details that could identify individuals.
- ☐ Delete or anonymise raw data after analysis unless retention is justified for audit/verification.

7.3 Publication and dissemination procedure

Before publishing deliverables, reports, educational materials, news items, photos, videos or social media posts, the responsible partner must confirm that the content is accurate, approved by the relevant WP leader, aligned with project visual identity and disclaimer requirements, free from unauthorised personal data, and compliant with IPR and licensing rules. Public deliverables should not include raw datasets, identifiable survey responses, private contact details or internal financial/confidential information unless publication has been explicitly approved and legally justified.

7.4 Data transfer between partners

Where possible, partners should transfer only aggregated or pseudonymised data. Raw personal data should remain with the collecting institution unless cross-partner processing is necessary for project purposes. When raw data must be shared, the responsible partners should document the purpose, recipients, security method, retention period and deletion plan. External transfers must comply with applicable data protection rules and institutional policies.

7.5 Monitoring and reporting

WP leaders should report significant data management or ethics issues in regular PMT reporting. The D1.2 lead may request short updates from partners on datasets collected, consent procedures used, incidents, pending risks and planned changes. The PMT will monitor whether DMP and ethics requirements remain appropriate and will propose updates when needed.

8 Monitoring, updates and conclusions

D1.2 establishes a practical and proportionate framework for responsible data management and ethical implementation in BOOSTSCIENCE. It supports compliance, transparency, accountability and trust between partners and stakeholders. Because the project will develop educational materials, a VLE, surveys, evaluation tools and public dissemination outputs over several years, the plan must remain responsive to the project's evolving activities.

The consortium will update this DMP when new data processing activities, tools, risks, dissemination needs or ethical requirements emerge. By applying the procedures, templates and safeguards defined in this document, BOOSTSCIENCE will protect participants, support high-quality evidence generation, and maximise the reuse and sustainability of non-sensitive project outputs.

Annex 1. Data inventory template

Field	To be completed by responsible partner
Dataset name	
WP/task/activity	
Responsible partner and contact	
Purpose of collection	
Target participants/data subjects	
Data categories collected	
Personal data? If yes, specify	
Sensitive/special category data?	
Lawful basis/consent procedure	
Tool/platform used	
Storage location	
Access rights	
Data sharing/transfer	
Retention period	
Anonymisation/pseudonymisation method	
Planned dissemination	
Deletion/archive date	

Annex 2. Participant information sheet and consent form template

Activity title: [insert title]

Project: BOOSTSCIENCE - Boosting Education Quality and Entrepreneurial Mindsets for Natural Sciences in Ukraine, Grant Agreement No. 101237769

Responsible partner/contact: [insert name, institution, email]

Purpose of the activity: [explain why the survey/interview/feedback is being conducted and how results will be used]

What participation involves: [describe questions, estimated time, whether recording/photo is involved, and any optional parts]

Voluntary participation: Participation is voluntary. You may refuse to participate or withdraw where feasible without negative consequences. If you are a student, your decision will not affect your grades, access to the module or relationship with the university.

Data collected: [list categories of personal and non-personal data]

Use of data: Data will be used for project analysis, reporting, quality improvement and dissemination. Public results will be presented in anonymised or aggregated form unless you explicitly consent to being identified.

Storage and access: [explain secure storage, access, retention and deletion]

Contact and rights: [insert contact for questions, withdrawal, data access/correction/deletion requests where applicable]

Consent statements:

- ☐ I confirm that I have read and understood the information above.
- ☐ I understand that my participation is voluntary.
- ☐ I consent to the processing of my data for the purposes described above.
- ☐ I consent to audio/video recording. [optional - delete if not applicable]
- ☐ I consent to the use of identifiable quotes/photos/videos for project communication. [optional - delete if not applicable]

Participant name/signature or electronic confirmation: _____ Date: _____

Annex 3. Short privacy notice template for online surveys

This survey is conducted within the BOOSTSCIENCE project (Grant Agreement No. 101237769). The purpose is [insert purpose]. The survey is voluntary. It will take approximately [insert time] minutes. We will collect [insert data categories]. Results will be analysed by [insert partner/team] and reported only in anonymised or aggregated form. Raw data will be stored securely and accessed only by authorised project staff. Data will be retained until [insert period] and then anonymised or deleted. By continuing, you confirm that you have read this notice and agree to participate. For questions, contact [insert contact].

Annex 4. Ethics and gender screening checklist

Question	Yes/No/NA	Comments/ action required
Does the activity involve human participants?		
Does the activity collect personal data?		
Are all data fields necessary for the stated purpose?		
Is a privacy notice provided before data collection?		
Is informed consent required and documented?		
Are participants informed that participation is voluntary?		
Could students feel pressured to participate because of teacher/student relations?		
Does the activity avoid sensitive data unless strictly justified?		
Is there any security-sensitive information related to Ukraine/war context?		
Is gender data collected only when relevant, optional and proportionate?		
Are inclusion/accessibility needs considered?		
Are raw data stored securely with restricted access?		
Will results be anonymised or aggregated before dissemination?		
Have IPR/copyright issues been checked before publication?		
Is escalation to D1.2 lead, PC, DPO or SC required?		

Annex 5. Data incident reporting form

Field	Information
Date/time discovered	
Reporting person and partner	
Activity/WP affected	
Type of incident	Loss / unauthorised access / accidental disclosure / wrong recipient / malware / publication error / other
Description of what happened	
Data affected	
Number/category of individuals affected	
Immediate containment actions	
People informed	WP leader / D1.2 lead / PC / institutional DPO / other
Risk assessment	Low / medium / high; explain
Corrective and preventive actions	
Closure date and responsible person	

Annex 6. VLE and learning analytics register

Field	Description
VLE platform/tool	
Administrator/responsible partner	
User groups	Students / teachers / administrators / external experts
Data collected	Registration, enrolment, login/access, quiz results, grades, completion, feedback, other
Purpose	Course delivery, learning support, evaluation, reporting, quality improvement
Access rights	
Data export rules	Only authorised exports; pseudonymise/aggregate for project reporting
Retention period	
Student information/notice provided	Yes/No; location of notice
Security measures	