



GLACY

Global Action on Cybercrime
Action globale sur la cybercriminalité

Version 22 September 2014

Guidelines for the delivery of Council of Europe judicial training courses on cybercrime and electronic evidence

Prepared under the GLACY project by
Nigel Jones (UK), Estelle De Marco (France),
Esther George (UK) and Adel Jomni (France)

www.coe.int/cybercrime

Funded
by the European Union
and the Council of Europe



EUROPEAN UNION

COUNCIL OF EUROPE



CONSEIL DE L'EUROPE

Implemented
by the Council of Europe

Contents

EXECUTIVE SUMMARY

1 INTRODUCTION AND BACKGROUND.....	5
2 HOW TO USE THE INTRODUCTORY AND ADVANCED COURSES	6
2.1 Introductory Course	7
2.1.1 The structure of the course.....	7
2.1.2 Course Requirements.....	7
2.1.3 Student requirements	8
2.1.4 Trainer requirements	8
2.1.5 Other considerations.....	9
2.2 Advanced Course	10
2.2.1 The structure of the course.....	10
2.2.2 Course requirements	10
2.2.3 Student requirements	11
2.2.4 Trainer requirements	11
2.2.5 Other considerations.....	12
3 TRAINING SKILLS COURSE	13
3.1.1 The structure of the course.....	13
3.1.2 Course Requirements.....	13
3.1.3 Student requirements	13
3.1.4 Trainer requirements	13
3.1.5 Other considerations.....	14
4 TIMETABLES AND PRACTICAL CONSIDERATIONS	15
4.1 Course Timetables	15
4.1.1 Timetable for Introductory Cybercrime and Electronic Evidence Course	15
4.1.2 Timetable for Advanced Cybercrime and Electronic Evidence Course	16
4.1.3 Timetable for 2-Day Training Skills Course.....	17
4.1.4 Combined timetable for Training Skills and Introductory Cybercrime and Electronic Evidence Courses	18
4.2 Templates.....	19

Contact

Cybercrime Programme Office of the
Council of Europe (C-PROC)
Tel +33-3-9021-4506
+40-21-201-7887
Email alexander.seger@coe.int

Disclaimer

This technical report does not necessarily reflect
official positions of the Council of Europe or the
European Union.

EXECUTIVE SUMMARY

This document is intended to provide guidance to those who will be delivering training that has been developed by the Council of Europe (COE)¹ to enhance the knowledge and skills of judges and prosecutors in the area of cybercrime and electronic evidence.

Previous COE projects have developed a number of training products that are available to support countries in their attempts to introduce sustainable training for the judiciary. The COE does not support the delivery of one off training courses, as these do not provide suitable long lasting benefits.

The COE approach is to work with countries to identify their needs and then work with them, to create a cadre of in country trainers that are able to deliver courses as part of a documented training strategy for judicial training. Sustainable training programmes are the only effective manner of ensuring that judges and prosecutors have sufficient knowledge to fulfil their roles effectively. The changing nature of cybercrime and electronic evidence requires that judicial staff undertake learning throughout professional development programmes, during their service and after introductory training during their initial training programme.

The concept of the COE is to empower countries to develop their own programme by providing the first levels of training and then supporting countries as they incorporate the available training into their programmes.

This paper provides information about the available training in order that it may be delivered during and following the involvement of the COE in each country. The report does not repeat the content of the existing material and provides references to that material in order that readers may consider them in conjunction with the information provide herein.

¹ Including under joint projects with the European Union.

1 INTRODUCTION AND BACKGROUND

The purpose of this document is to provide guidance to trainers who will be delivering training to judges and prosecutors on cybercrime and electronic evidence by making use of materials developed by the Council of Europe.

The training courses detailed in this document are available to any country seeking to improve the knowledge and skills of judges and prosecutors in relation to cybercrime and electronic evidence. They have been prepared with all the materials needed to run the courses. They consist of a training that includes:

- A training manual that includes an outline of the course and all the information needed to prepare for the course,
- Lesson plans that set out the aim and objective of each lesson together with information to assist trainers to deliver them,
- A draft and suggested timetable for the delivery of the course,
- Supporting materials, where appropriate, such as video or other presentation materials, as well as exercise sheets and a draft evaluation form for the students to complete at the end of the course, to provide feedback to the trainers and to allow the content of the course to be improved for the future.

It is important to recognise the purpose of the short **training skills course**. This is to provide new trainers with basic skills to assist them in delivering one or more of the core courses. It does not provide a qualification as a trainer and anyone proposing to undertake the role of trainer on a full time or regular part time basis will need to undertake further learning in their own country to bring their ability to train others up to the level required by their organisations.

The training skills elements are, typically, in COE projects, incorporated into the 3-day introductory cybercrime and electronic evidence training course as a method of introducing selected trainers to the concept of training, as well as the content of the 3 day course that they will adapt for local use and be expected to deliver in their own country. This method has been successfully used in previous COE projects and provides countries with the ability to incorporate the COE courses within their own curriculum, with the bonus of having trainers in place. Examples of the suggested timetable for each of the courses are supplied in **Section 4.1** of this paper. They are provided in stand-alone form and also as a combination of the joining together of the introductory and training skills courses. It is of course, possible for countries to amend the timetables to suit their own needs, while, importantly ensuring that the aim and objectives of the course are met. For example, some previous deliveries have introduced the training skills elements on the first 2 days of the course and the cybercrime and electronic evidence elements on days 3 to 5.

There now follows a breakdown of each of the COE courses. This includes a brief description of the materials available, the structure of each course and other considerations, such as information needed by trainers to deliver the courses and student prerequisites. In addition, further information is included that will help the smooth running of the courses. In **Section 4.2**, templates have been provided to ensure consistency of presentations and class layouts.

Some of the training materials are available at www.coe.int/cybercrime.

For full access to materials and additional information please contact nadia.bollender@coe.int

2 HOW TO USE THE INTRODUCTORY AND ADVANCED COURSES

The existing training materials are composed of three modules: an introductory course, an advanced course and a short training skills course. Each of these modules have separate and complementary objectives, and have been designed independently and supportively of each other.

As previously mentioned it is usual to incorporate the training skills course of 2 days, with the 3 day introductory cybercrime and electronic evidence course, to create a 5-day, train the trainers course. The structure of this course may be adapted to include training skills lessons between introductory course lessons, and as a result to obtain the five-days of training that addresses, each day, both training modules.

The advanced course, for its part, should be organised at a second stage, once the introductory course and the training skills course are completed and mastered by the future trainers.

The course material for each course is divided into the following:

- Training Manual
- Timetable,
- Lesson Plans,
- Presentations,
- Supporting Materials.

The training manual is the most important document as this sets out the rationale behind the course and explains why it has been created, as well as providing all the information needed to undertake delivery of the course locally. In order to identify the relevant documents, the timetable is divided into lesson numbers. The format uses three numbers divided by period marks, for example 1.1.1 or 1.1.2. The first number is the week of the course, to cater for courses that may be longer than one week, the second number is the day of the course and the third number the lesson number.

Each element of the training material follows this format to assist the reader in identifying relevant materials for each lesson.

It is essential that a contact point in the country of the training delivery is provided for the trainers to communicate with. This contact point may have a crucial role in the success of the training. Ideally, contact points should assist the trainers in the preparation of the delivery of the course. Their tasks, to be performed in the hosting country, should be the following:

- Provide the trainer with the information that is necessary for an efficient delivery of the training,
- Set and validate the training dates and location,
- Supervise the selection of students,
- Prepare the final list of participants,
- Meet the trainer at his arrival at the venue, and check with him the classroom and material that is available,
- Assist in finding solutions, prior the beginning of the training, to potential problems encountered while checking the tools necessary for the proper conduct of the training,
- Act as liaison between the trainers and the participants. The objective is to ensure, every day, with the participants, that the training is taking place with no equipment issue or other difficulty,
- Participate in any debriefing given at the end of each day,
- Act as a relay for the participants once the training is completed. He would distribute the received documents (updated courses, aid, guidance etc),

- If so required, participate in meetings organised by the COE, with regard to improving the training.

2.1 Introductory Course

The introductory course on cybercrime and electronic evidence for judges and prosecutors is designed to last three days and should be undertaken at the time of their introductory training programme.

The aim of the course is to provide judges and prosecutors with an introductory level of knowledge on cybercrime and electronic evidence. The course provides legal as well as practical information about the subject matters and concentrates on how these issues impact on the day-to-day work of judges and prosecutors.

2.1.1 The structure of the course

The course is divided into 12 lessons, spread over three days.

Lessons titles are the following:

- 1.1.1 Course Introduction
- 1.1.2 Introduction to Cybercrime
- 1.1.3 Introduction to Technology
- 1.2.1 Daily review
- 1.2.2 Introduction to Technology
- 1.2.3 Cybercrime as criminal offence in domestic legislation
- 1.2.4 Procedural Law / Investigative Measures in Domestic Legislation
- 1.2.5 Introduction to Technology
- 1.3.1 Daily review
- 1.3.2 Gathering electronic evidence; procedural and investigative measures
- 1.3.3 Gathering electronic evidence; procedural and investigative measures
- 1.3.4 International Cooperation
- 1.3.5 Student Feedback and Course Closure

2.1.2 Course Requirements

2.1.2.1 Training room arrangement

To enable interactions both between students and the trainer and between students themselves, the training room should be prepared in accordance with the layout set out for this course in **Section 4.2**.

2.1.2.2 Equipment

For delivery of this course in a training room environment, the following equipment is necessary:

- A Room of suitable size for the anticipated number of students,
- PC/Laptop running Windows 7 and loaded with MS Office Professional,
- Projector and display screen,
- Internet access (if available),
- Computer hardware examples (if available),
- Video clip "Warriors of the Net",
- Budapest Convention on Cybercrime including explanatory report,
- Council of Europe Guide on Electronic Evidence. (The latest version may be found at http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Electronic%20Evidence%20Guide/default_en.asp),

- Whiteboard,
- Whiteboard pens (at least 2 each of blue, black, red and green),
- 2 Flipcharts with adequate paper,
- Student notepaper and pens,
- Stapler, hole punch and scissors,
- Blu tack or a similar product to allow for paper to be affixed to the walls temporarily.

2.1.3 Student requirements

This course is designed for delivery to judges and prosecutors during their initial training period. Therefore, no previous subject knowledge is assumed.

2.1.4 Trainer requirements

2.1.4.1 Identify trainers with appropriate skills

Two trainers are required to deliver this course. They should both have a good level of knowledge of cybercrime issues and trends, and previous experience as trainers with knowledge of teaching theory and practice is required. One of the trainers should have a technical or investigative background, to be able to explain technical issues to students. The other trainer should have a legal background and should have a good level of knowledge of the Budapest Cybercrime Convention and of cybercrime legislation in his or her country of origin.

2.1.4.2 Prepare the delivery of the training

The lessons that have been prepared provide the headlines/topics of presentations/lectures as well as detailed explanations to be made by the trainers. The course is designed to be amended and adapted to meet national requirements and, where necessary, to students' profiles, while ensuring that the course's aim and objectives are met. This will provide consistency of training modules across borders. In addition, as part of the materials' adaptation, trainers should consider introducing a number of exercises/discussions that will facilitate the learning experience of the participants in each country.

2.1.4.2.1 Update and adapt the course to specific needs

It is recommended that training developers ensure that the material they prepare is as up to date as possible and incorporate the latest technology issues and their impact on criminal behaviour as well as their impact on the legal, procedural and evidential rules within the jurisdiction where the training is to be delivered. Examples of technological changes that affect the criminal justice system are solid state storage of data and Web 2.0. These are important issues that require inclusion in training programmes as they become more prevalent. Students could be invited to participate by giving examples of local cases. Such an exchange maintains the students' concentration and allows feeding the course with local examples.

In addition, although this course has been developed as a generic, not country specific programme, it is important that trainers personalise their training materials to ensure a more effective delivery of the course material. The use of case studies to inform the learning is considered suitable for this type of training and is more in keeping with adult learning styles than purely didactic teaching. Use of physical examples of technology referred to and use of the Internet may also enhance learning. Specifically, the sessions on substantive and procedural law in domestic legislation have been prepared as exemplars of the type of information that should be incorporated at the national level. Where this training is delivered to an audience of a single country, it is essential that the trainer include the relevant local legislation, using the material on the Budapest Convention, provided in the COE materials, as the basis for the amendments. Where the introductory course is delivered as part of a COE Train the Trainer Course, the COE trainer should explain this to those that will deliver the course at the local level. The COE trainers should

also take these sessions as an occasion to give examples of the legislation of their country of origin, and students could be invited to participate by giving examples of their national law. It would be beneficial to prepare the delivery with a local legal specialist, to either already include in supporting materials the latest legal developments relating to cybercrime in the country of delivery, or at least establishing a list of the national texts that are applicable with, where necessary, an indication on the way these texts may be consulted or obtained.

Adapting the course to the local specific needs and to students' profiles may also mean to adapt the time spent on each slide and issue dealt with within the framework of the course. If suitable, it may also be possible to extend the proposed number of training hours scheduled for a training day, to have one extra hour available in case of need on a particular issue.

Finally, trainers could ideally prepare, taking into account students' profiles, a document including basic definitions and important resources to be read before the beginning of the course. This document could also include a test in the form of a Multiple Choice Questionnaire (MCQ) or Quiz, to enable students to evaluate their own level before the training.

2.1.4.2.2 Ensure that the learning objectives are being achieved

No assessment of student knowledge was requested or provided as a part of this pilot course. Countries implementing this training at the national level may wish to introduce assessment. In any event trainers should check the knowledge of students during the course, by questioning, quizzes or other methods to ensure that the learning objectives are being achieved.

Regarding specifically the course objectives, they have been written in a traditional manner that will allow trainers to use various teaching methods to achieve them. Based on this, specific lessons' objectives have been set (and are available in the training manual), and these should be read in conjunction with the overall aim of the course.

2.1.4.2.3 Prepare the arrival at the venue

Trainers should arrive at the venue at least a day before the training, to check that everything is available and working for the training.

2.1.5 Other considerations

Trainers must be identified in advance to ensure their availability to deliver the training course and to prepare the course delivery.

To ensure a proper preparation of the training course, trainers should be provided with:

- The training material at least 12 weeks before the course,
- Details of the student's names and positions at least six weeks before the course, to enable the adaptation of materials to participants' profiles
- A contact point in the country of the training delivery.

Ideally, trainers should also be provided with a legal contact point in the country of the training, who would accept to help in the inclusion in the training materials of elements of the cybercrime legislation of the country of delivery, or at least in the elaboration of the list of applicable national legal texts.

2.2 Advanced Course

The Advanced course is designed as a 2-day course for judges and prosecutors as part of their initial or in-service training programme once they have successfully completed the basic cybercrime and electronic evidence course (or equivalent).

The aim of the advanced course is to provide the knowledge and skills to allow judges and prosecutors to fulfill their roles relating to cybercrime investigations and further develop the learning outcomes of the basic cybercrime electronic evidence course. The advanced course does this by enhancing judges and prosecutor's knowledge of the nature of cybercrime, the terms and the technology by dealing with a practical case scenario from the initial complaint, through the investigation and to the trial process.

2.2.1 The structure of the course

The course covers the following subjects:

- Conducting an investigation,
- Identifying the types of crime committed,
- Establishing the location of evidence, witnesses and suspects,
- Securing evidence in an acceptable way, irrespective of where it is held,
- Preparing for search and seizure activities involving electronic evidence,
- Dealing with digital devices that are part of the investigation,
- Briefing of forensic specialists and others needed to support the investigation phase,
- Preparing for interviews with suspects,
- Presenting cybercrime evidence,
- Considering the relevant aspects during the judicial process and trial.

A detailed scenario was created using the timeline that was relevant to the first delivery of this course. The email messages used are genuine and were created over a period of time to create authenticity and the opportunity for the students to conduct real time investigations using available Internet resources. In addition, a series of bank accounts were created as supporting material. These use genuine banks and branches to allow students to again use online resources to map the withdrawal of funds to support their investigation. The purpose is to create an awareness of the ability to conduct investigations using online resources as well as using the international cooperation mechanisms that often take far too long to be completed. The current materials are included as a template to serve only as the basis for the training of judges and prosecutors and not as the final goal for their training. Project countries/areas should discuss the needs at the national level and request additional specific training in the areas of cybercrime that they identify as most critical.

This course is very interactive and will require a great deal of investigation work on the part of the students as well as the provision of high levels of support from the trainers on the course.

2.2.2 Course requirements

2.2.2.1 Training room arrangement

The course as currently structured should be delivered in classroom setting using classroom based trainer instruction and practical paper feed exercises. It is recommended that the student group is divided into working groups of not more than 6 people for the entire course. The training room should be prepared in accordance with the layout set out for this course in **Section 4.2**.

2.2.2.2 Equipment

The following equipment is necessary:

- A room of suitable size for the anticipated number of students. This should be set up utilising one round table per team, where possible,
- PC/Laptop running Windows 7 and loaded with MS Office Professional,
- Projector and display screen,
- Internet access (if available),
- Computer hardware examples (if available),
- Copy of the Council of Europe Electronic Evidence Guide,
- Whiteboard,
- Whiteboard pens (at least 2 each of blue, black, red and green),
- 2 Flipcharts with adequate paper,
- Student notepaper and pens,
- Stapler, hole punch and scissors,
- Blu tack or a similar product to allow for paper to be affixed to the walls temporarily,
- One laptop per student team with similar set up to the trainer PC and with Internet access to allow for investigative research to be undertaken,
- All supporting material is provided with the training pack.

2.2.3 Student requirements

This Training Module is designed to be attended only by those judges and prosecutors that have already completed the introductory cybercrime and electronic evidence training course, designed by the Council of Europe, or its national equivalent.

2.2.4 Trainer requirements

2.2.4.1 Identify trainers with appropriate skills

Judicial training centres should employ trainers for this course and should include trainers with experience of conducting cybercrime investigations as well as being responsible for the prosecution and adjudication of such cases. Trainers should have a good level of knowledge of cybercrime issues/ trends and cybercrime legislation in their country of origin. Previous experience as trainers with knowledge of teaching theory and practice is required.

Trainers required for the advanced course are:

- Course manager who will be in charge of the course,
- An investigator,
- A forensic expert,
- A judge, and
- An expert or specialist on international cooperation.

2.2.4.2 Prepare the delivery of the training

Due to the nature of this course and its reliance on a developing scenario, it is vital that the trainers take sufficient time to make themselves aware of the content of the course and prepare for delivery. Trainers should ensure that the material they prepare is up to date and incorporates the latest technology issues as they impact on criminal behaviour; its impact on the legal, procedural and evidential rules within the jurisdiction where the training is to be delivered.

Trainers could ideally prepare, taking into account students' profiles, a document including the important notions from the basic course that must imperatively be known. This document could also include a test in the form of a Multiple Choice Questionnaire or Quizz, to enable students to evaluate their own level before the training, to ensure this level meets the requirements of the advanced course.

2.2.4.2.1 Update and adapt the course to specific needs

This course has been designed as a mixture of taught lessons and a practical scenario, taken from the first report of the crime through to the preparation of the case for court. The presentations complement the learning created during the practical scenario. The scenario was time specific and will require updating to make it relevant to the period of time in which it is being delivered. It may also be adapted so that the victim company resides in the country in which the course is delivered, in order to make the criminal and procedural legislation more relevant. It is therefore recommended that the trainers have at least three months to replicate all the evidence for the course and in order for the supporting materials to be updated to make them timely.

The lessons that have been prepared provide the headlines/topics of presentations/lectures as well as detailed explanations to be made by the trainers. The course is designed to be amended to meet national requirements, while ensuring that the course aim and objectives are met. This will provide consistency of training modules across borders. Trainers should consider introducing a number of exercises/discussions which will facilitate the learning experience of the students in each country.

The scenario resources were developed in 2012 and it may be necessary to update some of the messages and bank statements in particular, to make them relevant to the time period in which the course is being delivered. It is the responsibility of the trainer, in conjunction with the training organisation commissioning the course, to ensure its relevance to the audience.

2.2.4.2.2 Ensure that the learning objectives are being achieved

No assessment of student knowledge was requested or provided as a part of this pilot course. Countries implementing this training at the national level may wish to introduce assessment. In any event trainers should check the knowledge of students during the course, by questioning, quizzes or other methods to ensure that the learning objectives are being achieved.

Regarding specifically the course objectives, they have been written in a traditional manner that will allow trainers to use various teaching methods to achieve them. Based on this, specific lessons' objectives have been set (and are available in the training manual), and these should be read in conjunction with the overall aim of the course.

2.2.4.2.3 Prepare the arrival at the venue

It is suggested that trainers should arrive at the venue at least a day before the training, to check that everything is available and working.

2.2.5 Other considerations

The trainers should have a contact point in the country of the training and should be sent details of the student's names and positions at least two weeks before the course.

3 TRAINING SKILLS COURSE

The training skills course aims at providing judges and prosecutors who have specific responsibility for cybercrime investigations, prosecutions and adjudications, with practical skills to enable them to function effectively as trainers.

3.1.1 The structure of the course

The course covers the following subjects:

- Identifying the characteristics of good and poor presenters,
- Giving and receiving feedback,
- Verbal and non verbal communication,
- Preparation and planning,
- Training delivery mechanisms,
- Audience engagement,
- Questioning and Listening,
- Students will also deliver a prepared presentation and receive feedback from participants and trainers.

3.1.2 Course Requirements

3.1.2.1 Training room arrangement

To enable interactions between students, the training room should be prepared in accordance with the layout set out for this course in **Section 4.2**.

3.1.2.2 Equipment

For delivery of this course in a training room environment, the following equipment is necessary:

- A Room of suitable size for the anticipated number of students,
- PC/Laptop running Windows 7 and loaded with MS Office Professional,
- One printer connected to the trainers computer,
- Projector and display screen,
- Internet access (if available),
- Whiteboard,
- Whiteboard pens (at least 3 each of blue, black, red and green),
- Flipchart with adequate paper,
- Student notepaper and pens,
- Stapler, hole punch and scissors,
- Blu tack or a similar product to allow for paper to be affixed to the walls temporarily.

3.1.3 Student requirements

This course is designed for delivery to judges and prosecutors as part of their training development programme. No previous knowledge of training methodology or experience is assumed.

3.1.4 Trainer requirements

3.1.4.1 Identify trainers with appropriate skills

The Trainers for pilot deliveries of this course will be international experts appointed by the Council of Europe. Further delivery should be conducted by those employed by national judicial training centres where this training will be delivered.

Trainers should have a good level of knowledge of training methodology. Previous experience as trainers with knowledge of teaching theory and practice is required.

3.1.4.2 Prepare the delivery of the training

The lessons that have been prepared provide the headlines/topics of presentations/lectures as well as detailed explanations to be made by the trainers. The course is designed to be amended and adapted to meet national requirements, while ensuring that the course's aim and objectives are met. This will provide consistency of training modules across borders. In addition, as part of the materials' adaptation, trainers should consider introducing a number of exercises/discussions that will facilitate the learning experience of the participants in each country.

3.1.4.2.1 Update and adapt the courses to specific needs

It is recommended that training developers ensure that the material they prepare is as up to date as possible.

In addition, it is important that trainers personalise their training materials to ensure a more effective delivery of the course material. The use of case studies to inform the learning is considered suitable for this type of training and is more in keeping with adult learning styles than purely didactic teaching.

3.1.4.2.2 Ensure that the learning objectives are being achieved

No assessment of student knowledge was requested or provided as a part of this pilot course. In any event trainers should check the knowledge of students during the course, by questioning, quizzes or other methods to ensure that the learning objectives are being achieved. This module does have the opportunity for students to deliver a short training presentation and receive feedback from trainers and other participants.

Regarding specifically the course objectives, the key role of the training developer is to ensure the overall aim of any learning event and the specific objectives are achieved. The manual provides some information to assist that process.

3.1.4.2.3 Prepare the arrival at the venue

Trainers should arrive at the venue at least a day before the training, to check that everything is available and working for the training.

3.1.5 Other considerations

3.1.5.1 Trainers' preparation

Trainers must be identified in advance to ensure their availability to deliver the training course and to prepare the course delivery.

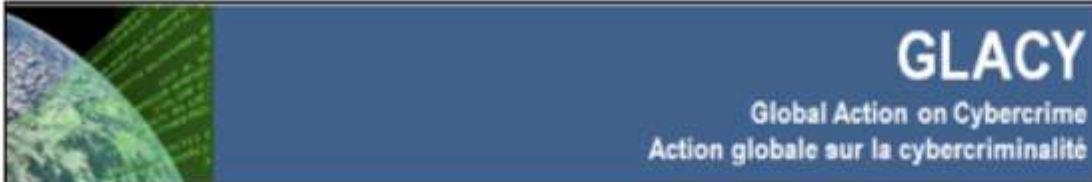
To ensure a proper preparation of the training course, trainers should be provided with:

- The training material at least 12 weeks before the course,
- Details of the student's names and positions at least six weeks before the course.

4 TIMETABLES AND PRACTICAL CONSIDERATIONS

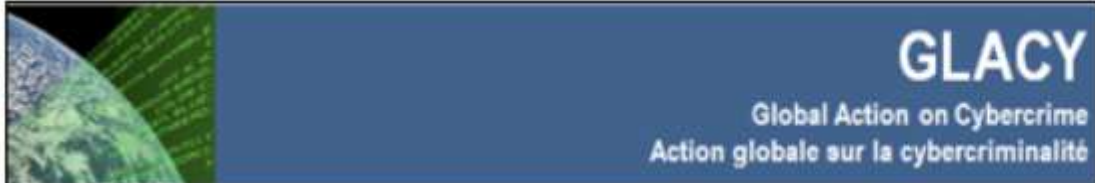
4.1 Course Timetables

4.1.1 Timetable for Introductory Cybercrime and Electronic Evidence Course

																Council of Europe Judicial Training Cybercrime and Electronic Evidence Course Proposed TIMETABLE	
		08:00-08:30	08:30-09:00	09:00-09:30	09:30-10:00	10:00-10:30	10:30-11:00	11:00-11:30	11:30-12:00	12:00-12:30	12:30-13:00	13:00-13:30	13:30-14:00	14:00-14:30	14:30-15:00		
Day 1		1.1.1 Course Opening and Introductions Ice Breaker <i>1.5hrs</i>		BREAK	1.1.2 Introduction to Cybercrime Threats, Trends and Challenges <i>2hrs</i>				LUNCH BREAK		1.1.3 Introduction to Technology Part 1 <i>1.5hrs</i>		BREAK	1.1.3 Introduction to Technology Part 2 <i>1hr</i>			
Day 2	1.2.1 Daily Review <i>30 min.</i>	1.2.2 Introduction to Technology Part 3 <i>1.5hrs</i>			BREAK	1.2.3 Cybercrime Legislation Substantive Articles of the Budapest Convention on Cybercrime <i>1.5hrs</i>			LUNCH BREAK		1.2.3 Cybercrime Legislation Substantive Articles of the Budapest Convention on Cybercrime <i>(continued) 1 hr</i>	BREAK	1.2.4 Cybercrime Legislation Procedural Articles of the Budapest Convention on Cybercrime <i>1.5hrs</i>				
Day 3	1.3.1 Daily Review <i>30 min.</i>	1.3.2 Electronic Evidence Practice and Procedure <i>1.5hrs</i>			BREAK	1.3.2 Electronic Evidence Practice and Procedure <i>1.5hrs</i>			LUNCH BREAK		1.3.3 International Cooperation <i>1.5hrs</i>		BREAK	1.3.4 Delegate Feedback and Course Closure <i>1hr</i>			

NB---Other breaks will be taken at appropriate times during each day of training.

4.1.2 Timetable for Advanced Cybercrime and Electronic Evidence Course

		Council of Europe Judicial Training Advanced Cybercrime & Electronic Evidence Course Proposed TIMETABLE													
		08:00-08:30	08:30-09:00	09:00-09:30	09:30-10:00	10:00-10:30	10:30-11:00	11:00-11:30	11:30-12:00	12:00-12:30	12:30-13:00	13:00-13:30	13:30-14:00	14:00-14:30	14:30-15:00
Day 1	1.1.1 Course Opening and Introductions Ice Breaker 1hr	1.1.2 Developing an Investigation Presentation 1 hr	1.1.3 Identifying Crimes, Developing an Investigation Plan Group Work 2 hrs			LUNCH BREAK			1.1.4 International Cooperation Presentation 1 hr	1.1.5 International Cooperation Group Work 1 hr	1.1.6 Identifying Suspects & Planning Arrest Strategy Group Work 1 hr				
Day 2	1.2.1 Daily Review 30 min.	1.2.2 Digital Forensics Parts 1 & 2 2 hrs			1.2.3 Digital Evidence Needs, Jurisdiction & International Issues Group Work 1.5 hrs			LUNCH BREAK			1.2.4 Preparing the Case for Court Presentation 1 hr	1.2.5 Finalising the Case Group Work 1 hr	1.2.6 Case Review, Delegate Feedback & Course Closure 1 hr		

NB--Other breaks will be taken at appropriate times during each day of training.

4.1.3 Timetable for 2-Day Training Skills Course

		Council of Europe Judicial Training Training Skills Course Proposed TIMETABLE													
		08:00-08:30	08:30-09:00	09:00-09:30	09:30-10:00	10:00-10:30	10:30-11:00	11:00-11:30	11:30-12:00	12:00-12:30	12:30-13:00	13:00-13:30	13:30-14:00	14:00-14:30	14:30-15:00
Day 1	1.1.1 Course Opening and Introductions Ice Breaker 1hr	1.1.2 Training Skills Good Presenter/Poor Presenter Giving and Receiving Feedback Controlling your Nervousness 1.5 hrs			1.1.3 Training Skills Verbal and Non Verbal Communication 1.5 hrs			LUNCH BREAK		1.1.4 Training Skills Preparation Presentations and Other Delivery Techniques 1.5hrs			1.1.5 Training Skills Audience Engagement Questioning and Listening 1.5hrs		
Day 2	1.2.1 Daily Review 30 min.	1.2.2 Delegate Presentations on Chosen Subjects 3.5hrs						LUNCH BREAK		1.2.2 Delegate Presentations on Chosen Subjects 1.5hrs			1.2.3 Module Feedback from Delegates and Trainers 1 hr		1.2.4 Course Closure 30 Mins

NB--Other breaks will be taken at appropriate times during each day of training.

4.1.4 Combined timetable for Training Skills and Introductory Cybercrime and Electronic Evidence Courses

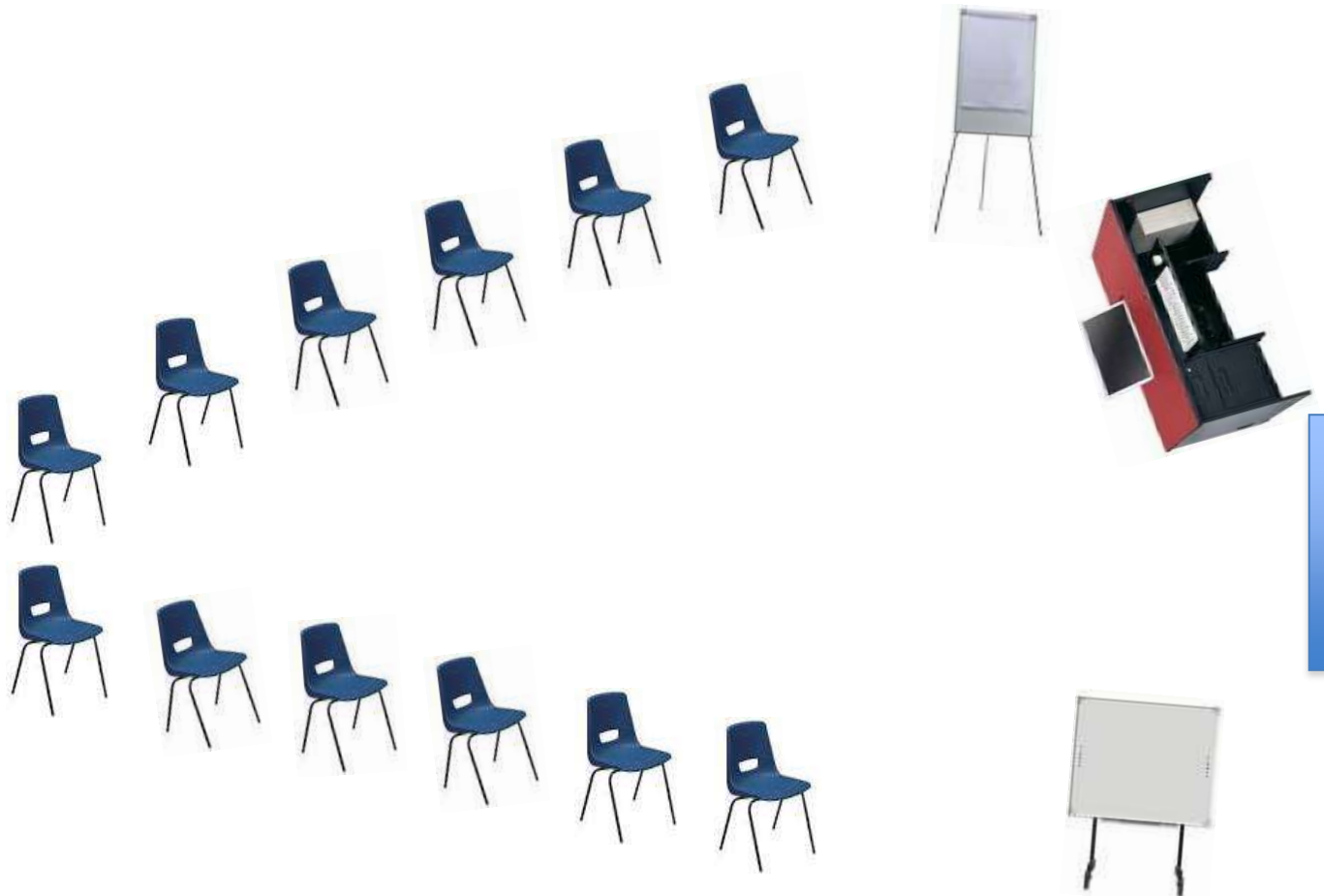
												Council of Europe Training for Trainers Cybercrime and Electronic Evidence Course Proposed TIMETABLE				
		08:00-08:30	08:30-09:00	09:00-09:30	09:30-10:00	10:00-10:30	10:30-11:00	11:00-11:30	11:30-12:00	12:00-12:30	12:30-13:00	13:00-13:30	13:30-14:00	14:00-14:30	14:30-15:00	15:00-15:30
Day 1		1.1.1 Course Opening and Introductions Ice Breaker 1.5hrs		BREAK	1.1.2 Training Skills Good/Poor Presenter Giving/Receiving Feedback 2hrs			LUNCH BREAK	1.1.3 Cybercrime Threats and Challenges 1.5hrs		BREAK	1.1.4 Technology for Judges and Prosecutors (1) 1hr		National Adaptation of Materials		
Day 2	1.2.1 Daily Review 30 min.	1.2.2 Training Skills Verbal and Non Verbal Communication 1.5hrs		BREAK	1.2.3 Cybercrime Legislation Substantive Articles of the Budapest Convention on Cybercrime 1.5hrs			LUNCH BREAK	1.2.4 Cybercrime Legislation Substantive Articles of the Budapest Convention on Cybercrime 1.5hrs		BREAK	1.2.5 Technology for Judges and Prosecutors (2) 1hr		National Adaptation of Materials		
Day 3	1.3.1 Daily Review 30 min.	1.3.2 Training Skills Presentations and other delivery techniques preparation 1.5hrs		BREAK	1.3.3 Cybercrime Legislation Cybercrime Legislation Procedural Articles of the Budapest Convention 1.5hrs			LUNCH BREAK	1.3.4 Cybercrime Legislation Cybercrime Legislation Procedural Articles of the Budapest Convention 1.5hrs		BREAK	1.3.5 Technology for Judges and Prosecutors (3) 1hr		National Adaptation of Materials		
Day 4	1.4.1 Daily Review 30 min.	1.4.2 Training Skills Audience Engagement Questioning and Listening 1.5hrs		BREAK	1.4.3 Electronic Evidence and Practices International Standards and Good Practice Guides 1.5hrs			LUNCH BREAK	1.4.4 International Cooperation Provisions of the Budapest Convention and other mechanisms 1.5hrs		BREAK	1.4.5 Preparation for Delegate Presentations 1hr		National Adaptation of Materials		
Day 5	1.5.1 Daily Review 30 min.	1.5.2 Delegate Presentations on Chosen Subjects All delegates will give a 20 min lesson on one of the course subjects- 3.5 hrs					LUNCH BREAK	1.5.2 Delegate Presentations on Chosen Subjects All delegates will give a 20 mins lesson on one of the course subjects (continued) 1.5hrs		1.5.3 Feedback from Delegates and Trainers 1hr		1.5.4 Course Closure 30 mins		National Adaptation of Materials		

NB—Other breaks will be taken at appropriate times during each day of training.

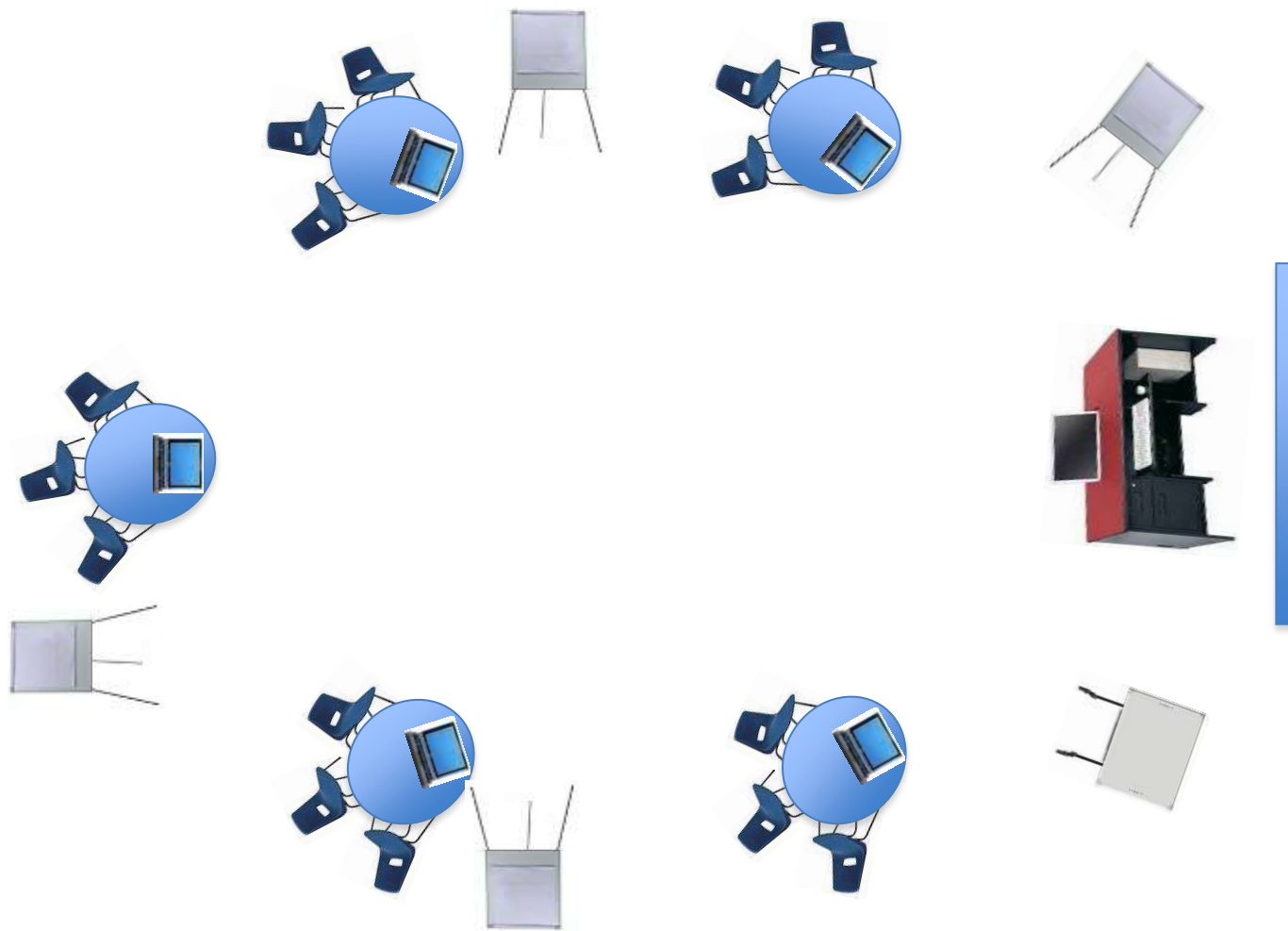
4.2 Templates

Classroom Layouts

3-Day Introductory Cybercrime and Electronic Evidence Course, 2-Day Training Skills Course and 5-day combination of both courses



Advanced Cybercrime and Electronic Evidence Course



Template Presentation slides for all courses



Name of Training Course Here

Session X.X.X.

(TOPIC)

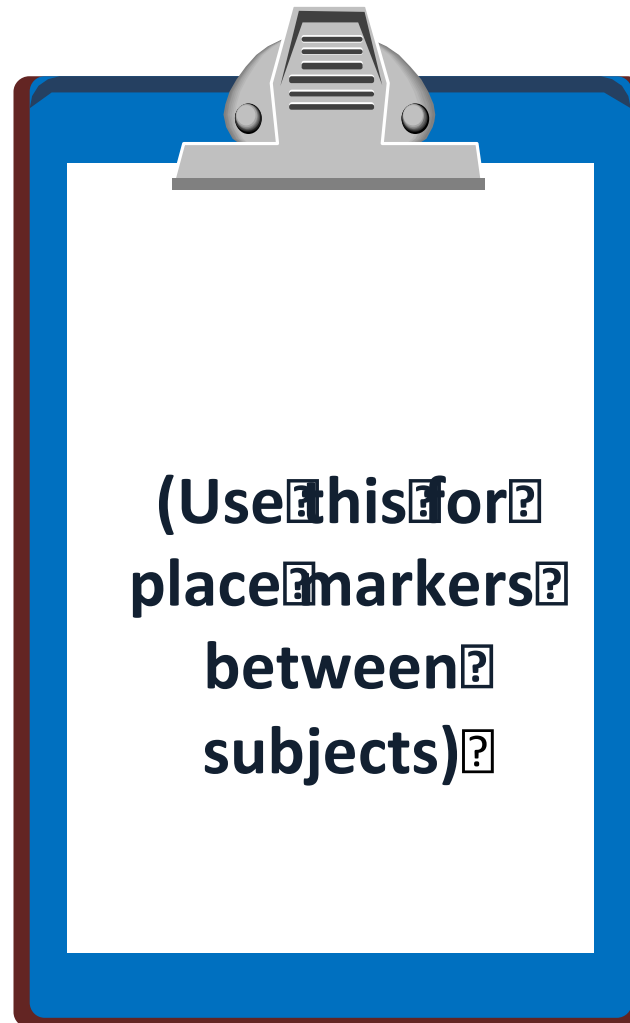
Session Objectives

At the end of this session participants will be able to:

- (list SMART objectives of the session here)
-
-
-
-
-
-

(Slide Heading)

- This is the slide for text use in presentations



(Slide Heading)

- This is the slide for text use in presentations

Summary of Session Objectives

At the end of this session participants will be able to:

- (Repeat Session objectives here as a reminder of what has been taught during the session)



Questions?