Data Use and Security Guidelines

Users of Carlow College personal data, including employees and learners, must comply with these guidelines. This is not intended to be an exhaustive list of safeguards. Further measures may be in place regarding technical security in the policies of IT Services. While the Data Protection Policy refers to personal data, these guidelines are also valuable to protect non-personal College records.

Collecting and creating records

- Double check your recipient when sending emails.
- Password-protect email attachments containing personal data and confidential business information. Additionally, the document sharing facilities in Office 365 / MS Teams can be used to share files. Do not email the password. Communicate it by a different means e.g. text message or phone call.
- Do not collect personal data unless it is required e.g. make surveys anonymous.
- Official records should be kept in the College's electronic or manual systems.
- Use College devices, where possible.
- If it is necessary to use a personal device, particularly a shared device, ensure that College records are kept securely and confidentially.
- Do not use personal accounts to create or store official records.
- If personal accounts/devices must unavoidably be used, copy records to College systems/devices as soon as possible and delete them from personal accounts/devices.
- Keep personal data up to date and make requested changes promptly e.g. change contact details on request.
- While straightforward updates may be made e.g. change of address on a system, do not alter a document created by another employee without their permission.
- Personal data is not to be posted on public noticeboards or other public spaces.
- When recording personal data, check back with data subjects that what you have recorded is accurate, when appropriate e.g. send them a copy or read it back.
- Ensure that your communications are written in an objective, truthful, responsible and accurate manner.
- Pseudonymise or anonymise personal data, as appropriate, when it is no longer required to identify individuals.
- Carry out a Data Protection Impact Assessment (DPIA), where required.
- Consider data protection issues early in a new project and contact the DPO.
- Carry out audits on data quality e.g. check for errors.

- Design forms to collect the minimum personal data necessary to fulfil your purpose.
- Collect personal data in a privacy friendly manner e.g. sign-in books used by multiple persons to record their contact details might be replaced with individual use forms in paper or electronic formats.

Access

- Access permissions for both manual and IT systems should align with employee duties.
- Do not access records that you have not been authorised to view i.e. records unrelated to your duties or for which you have not been granted access permissions.
- Employees may have access to personal data in systems that they do not require e.g. about learners that they do not teach. Employees should only access personal they require to carry out their duties.
- Keep your password secure and private to you.
- Use robust passwords. They should contain a mixture of letters and other characters (see advice under 'Access Control' here).
- Change your passwords regularly.
- Do not use the same password for multiple accounts.

Respecting other people's privacy

- Photographs may be personal data. Ensure that you only use photographs in a manner allowed by Data Protection law. This may vary on the circumstances, but photographs require either consent or a legitimate interest (e.g. people would likely not be surprised to be photographed at a conferring ceremony). However, care should still be taken when deciding how to use photographs, and consideration given to what people might expect photographs would be used.
- If holding an event, inform attendees if photographs will be taken or the event recorded. This can be done by posting notices in the area, informing people when inviting them or during the booking process etc. Such notices can suggest that people speak to the photographer if they do not wish to be photographed. Notices should also indicate if it is intended to make photographs available e.g. on social media. The DPO can assist event organisers to draw up such notices.If an individual objects to the publication or other use of their photograph, comply with their wishes.
- Consider the data protection and privacy rights of others before you share an image or video of a video call that includes the image, voice or contact details of participants. Such sharing is discouraged.

- Covert recording of employees, learners or any other person with whom employees or learners come into contact in the workplace or through the course of duties of studies is not permitted.

Disclosing personal data

- Double check your recipient when sending an email.
- Password-protect email attachments containing personal data and confidential business information. Do not email the password. Communicate it by a different means e.g. text message or phone call.
- Send group emails via ‘bcc’ where it is not appropriate that recipients see each other’s email address e.g. external email addresses; marketing mailing lists; where membership of a group should not be disclosed to others e.g. Counselling clients.
- In general, employees are only to disclose learner personal to parents/guardians or other family members with the learner’s written consent. This applies to all data including about fees, attendance, grades etc. There are extremely limited exceptions to this i.e. in a life-and-death situation.
- References about learners should only be provided to prospective employers, other educational institutions etc with the learner’s consent.
- Student ID numbers are personal data as they are linkable to an individual. They cannot be used to anonymise information about learners.
- Share personal data and other records with colleagues on a need to know basis only.
- If authorised employees from other departments need to borrow files from your office, implement a sign in/out book. Agree a borrowing period and issue a reminder if not returned on time.
- Do not share personal data or other confidential information acquired through your official duties on social media.

Disposing of records

- Dispose of personal data and other confidential records securely. Shred paper records.
- Paper records are not to be disposed of in wastepaper or recycling bins.
- Return devices to IT Services for secure deletion of data and disposal.
- Dispose of records in accordance with the Records Retention Schedules.
- Some records are designated ‘archival’, which means that they are kept on an ongoing basis. Transfer them to the Delany Archive.

Keeping records secure

- All personal data and non-personal business records are confidential. Employees are to maintain and protect this confidentiality.
- Notify the DPO immediately of any incident where data has been put at risk or you suspect a potential or actual personal data breach or incident.
- Take appropriate methods to secure records when leaving your workspace e.g. lock your screen; lock the door; store paper records securely.
- Do not leave the key in your office door.
- Do not leave unauthorised people alone with personal data or other confidential business records.
- Keep records out of arm's reach to visitors.
- Do not allow your computer screen to be viewable from a public area or to an unauthorised person.
- Locked storage units are ideal for paper records.
- Do not remove records from the College premises unless necessary.
- Return borrowed records to the College as soon as you are finished with them.
- Do not leave records on view in your car or in your car overnight.
- Assignments and examination scripts are not to be corrected in a public place.
- Do not store records on removable devices, such as memory sticks, unless necessary
- Do not print unnecessary paper copies of documents.
- Do not leave personal data or other confidential records unattended at photocopiers or other public locations.
- Employees who are changing position or leaving the College's employment are to ensure that they leave all relevant records for their successor.

New colleagues and volunteers

- Appoint a 'buddy' to new employees to explain procedures for handling personal data and other records.
- Volunteers and people on work experience should have limited or no access to personal data and other confidential records.

System/software privacy

- Privacy Policies or Notices are available for many systems/software that are in use in Carlow College. They are generally found on the login page.
- Some systems/software allow users some user control over privacy settings e.g. what information is in a public profile. These controls are often found under the 'settings' tab.
- Further information may be sought from the relevant system administrator or the Data Protection Officer (DPO).

Working remotely

The protocols outlined below are particularly relevant to hybrid / remote working, but users should note that the Data Protection Policy applies in full at all times and locations where Carlow College personal data is processed. Advice about hybrid / remote working issued by the Data Protection Commission (DPC) has been incorporated here. As a general point, if particular arrangements have been put in place for you, ensure that you abide by them.

Workspace

Ensure that your workspace is sufficiently private to protect the confidentiality and security of data/records. Ideally, the workspace is occupied solely by the employee, and this is required during online meetings and phone calls.

Devices and Accounts

- Ensure that your computer, laptop or other device is used in a safe location where you can keep sight of it. Ensure that others cannot view the screen.
- Ensure that any device you use has the necessary updates, such as operating system updates (like iOS or Android) and software/antivirus updates.
- Ensure that your devices are turned off, locked and stored carefully, and sign out of work accounts when not in use or if you have to leave them at any point.
- Use effective access controls (such as multi-factor authentication and strong passwords) and, where available, encryption to restrict access to the device, and to reduce the risk if a device is lost or stolen. Passwords should contain a mixture of letters and other characters (see advice under 'Access Control' here).
- When a device is lost or stolen, take steps immediately to ensure a remote memory wipe, where possible.
- Where possible, only use the College's trusted networks or cloud services, and comply with any organisational rules and procedures about cloud or network access, login, and data sharing.
- Ensure that smart listening devices are turned off in work locations so that they do not collect work data. This includes devices such as Alexa and listening devices on phones.
- If you are working without cloud or network access, ensure any data stored locally is effectively backed up in a secure manner.
- Do not leave devices in plain sight when transporting them e.g. in the passenger compartment of your car.
- Use of portable storage devices such as USBs is not permitted, except in exceptional circumstances.

Electronic records

- If using a shared device, ensure that you are particularly careful about the security and confidentiality of personal data (and non-personal records). Sign out of work accounts when not working, ensure that your passwords are secure, and take care that data is not accessible to others. Avoid using the Downloads folder or saving files to your device's hard drive. Instead, save data within College systems.
- Even if you have sole use of a device, avoid using your Downloads Folder and saving data to your device's hard drive as far as possible. This applies to all devices, including your phone.
- Sensitive or special category personal data (e.g. health, disability, learning difference, religious beliefs, sex life, sexual orientation, trade union membership etc.) and other confidential information are not to be saved locally to any device. Instead, use College systems.
- If it is necessary in exceptional circumstances to use your Downloads folder or device's hard drive to store data, copy it to College systems as soon as possible and delete it from your device.
- Use work email accounts rather than personal ones for work-related emails. If you have to use personal email, ensure that contents and attachments are encrypted and avoid using personal or confidential data in subject lines. As soon as possible, copy the email to your work account and delete it from your personal account.

- Keep your own personal files separate to work files.
- Users are not permitted to use software/systems that have not been approved by Carlow College.

Paper records

- Employees should use electronic records rather than paper records, where possible, when working remotely.
- Ensure the security and confidentiality of paper records, taking particular care of special category personal data (e.g. health, disability, learning difference, religious beliefs, sex life, sexual orientation, trade union membership etc.)
- Confidential information and personal data should be kept in locked storage e.g. a locked office or filing cabinet.
- Paper records containing special category personal data should be removed from the office or created/held at remote working locations in exceptional circumstances only. If current routine processes stipulate paper records containing special category data, a change of process to make the work safer should be undertaken, or the task may be more suited to onsite completion. The same protocol applies to non-personal confidential records.
- Do not print records at home or at other remote working locations unless unavoidable.
- It is not permitted to carry paper records containing confidential information or personal data (including special category personal data) on public transport.
- Do not leave paper records in plain sight when transporting them e.g. in the passenger compartment of your car.
- Ensure that paper records are disposed of securely i.e. shred them. Do not put paper records in domestic refuse if they would normally be shredded onsite.
- Only remove paper records from the College premises when it is strictly necessary and return them to the College as soon as possible.
- Keep a written record of records and files that have been removed from the College premises in order to maintain good access and governance practices. Functions in which paper records are shared may find it useful to create a function-level register.

Personal data breaches

- The normal procedure for reporting personal data breaches applies during remote working i.e. report the matter to the DPO without delay, or to the President’s Office, Director of Operations or your line manager if you cannot reach the DPO.
- Personal devices may be used during remote (and onsite) work. Employees should report the loss/theft/compromising of personal data on any device that contains Carlow College personal data e.g. laptop, computer, phone, USB etc.

Suspicious communications

- Be extra vigilant about opening attachments or web links in emails, text messages or other messages. This applies to messages received from both familiar and unfamiliar senders.
- If you are uncertain about the authenticity of a message, verify it by contacting the organisation in question through established channels (e.g. official website).

- Be extra vigilant about sharing any individual's personal data (e.g. username, password, financial information), including your own, during phone calls or on foot of any type of message.
- If you are uncertain about a caller's identity, verify it by other means (e.g. official website, phone book, relevant College system) and call back.

Changing position/leaving Carlow College's employment

If you have used a personal device for work purposes and afterwards change position or leave the College's employment, you are obliged to certify in writing at the request of Human Resources that you have securely deleted all College personal data and other work records, apps etc from your devices. This includes laptop, computer, phone etc.

Disposing of personal devices used for work purposes

- If you have used a personal device for work purposes and are afterwards disposing of it, you are responsible for ensuring that personal data and other work records held on it are securely deleted. This includes laptop, computer, phone etc. Advice may be sought from IT Services.

Online Meetings and Events

Purpose

The purpose of these guidelines is to inform members of the Carlow College community about appropriate video conferencing use and etiquette. The terms 'meeting'/'business meeting' and 'event' are used throughout. The term 'meeting'/'business meeting' refers to any meeting that concerns the official business of Carlow College, and 'event' might refer to conferences, lectures, colloquia, open days, information sessions etc. Events may be attended by the College community and/or invited guests, and the general public.

Platforms

- Employees are to use Microsoft Teams for internal meetings.
- It may be more appropriate to use webinar rather than meeting settings for some events (e.g. public events), and Carlow College has a Zoom account that employees can avail of.
- Caution should be exercised when subscribing to any virtual platform, in particular, think about what permissions you are being asked for and whether they are necessary (e.g. your location; access to your contacts). The minimum information should be shared with platforms.
- Avoid sharing organisational data, document locations or hyperlinks when using any platform other than Microsoft Teams.
- Do not forward meeting invitations to other individuals. Instead, contact the meeting organiser to arrange the sharing of invitations.

Your device

- Ensure that your device has the necessary updates, including operating system and software updates.
- Ensure that your device is protected by antivirus software.
- Be conscious of what and who can be seen and heard from your camera. Protect the privacy of other people around you and those on the call. As appropriate, wear a

headset if you are in a shared space or where others may hear your call, or ensure that you are in a private space.

- If screen sharing, ensure that confidential data is not visible on screen and choose settings to ensure that pop ups such as emails do not appear on screen.
- Ensure that that you log out, mute your mic or turn off your camera (as appropriate) when leaving a meeting or taking a break from it.
- Consider the data protection and privacy rights of others before you share an image or video of a video call that includes the image, voice or contact details of participants. Such sharing is discouraged.

Recording business meetings

- In general, business meetings are not to be recorded. Where this is proposed, there should be an identified legitimate reason for recording, which should be notified in advance to all participants, as well as the intended uses and sharing of the recording.
- Covert recording refers to recording, audio or visual, carried out without the knowledge and consent of an individual(s). It includes recording on devices and systems of all types, including but not limited to, CCTV, phones and virtual meeting platforms. Employees and learners are not permitted to carry out covert recording of employees, learners or any person with whom they come into contact in the workplace or through the course of their duties or studies.
- Any covert recordings must have the prior approval of a representative group of senior management.
- Inform participants when beginning/ending recording.
- Recordings should not be kept for longer than is necessary to fulfil the purpose for which they were created.
- Recordings are potentially accessible under Data Protection and Freedom of Information laws, and via other legal processes.

Recording events

- It may be proposed to record events and make the recording available online. In such cases, recording and sharing are to be notified to participants when booking the event, and to speakers when they are invited to participate. There should always be a legitimate reason for recording an event and sharing that recording, whether online or by some offline means.
- Recordings should be reviewed by the event organiser prior to sharing the recording or making it available online. Where special category data is disclosed by any participant or where there may be legal implications (e.g. defamation), the recording should be edited to redact the data or a decision made not to share or publish the recording should be taken.
- Recordings are potentially accessible under Data Protection and Freedom of Information laws, and via other legal processes.
- Recordings should not be kept for longer than is necessary to fulfil the purpose for which they were created.

Hosting events

- It is the responsibility of the event organiser to make data protection information available to participants.
- Carlow College has an Events Privacy Notice, which should be made available to all participants at the time of booking (i.e. not after booking).

- The Events Privacy Notice should also be made available to proposed speakers when they are invited to participate in an event.
- The Events Privacy Notice is generic and cannot take account of details specific to individual events. Therefore, the event organiser should supplement the Events Privacy Notice with any further relevant information (e.g. if it is proposed to record the event; or make the recording available on the internet). This further information should be made available at the same time as the Events Privacy Notice.
- Instruct participants not to share invitations sent to them.
- Video conferencing platforms have various functionalities. Settings should be chosen to promote data security and data protection rights:
    - Restrict access to video calls to those who need to present. Do not publish meeting IDs or passwords.
    - If sensitive topics are being discussed, consider whether participants can ask questions anonymously. Do not mention the names of participants when answering their questions.
    - Mute participant mics and turn off participant cameras unless they require such permissions.
    - Control when people can join the call and who is allowed to share their screen.