Handling Information in Line with Classification

All staff handling Council information assets and computing / IT equipment are responsible for the appropriate protection of that asset. The instructions provided are for the most common handling scenarios used by staff in normal circumstances. If you have a scenario that is not listed or believe your circumstances mean exceptions apply, contact Information Security via e-mail at information.security@eastrenfrewshire.gov.uk to discuss appropriate options.

Handling	Handling Instructions OFFICIAL	Handling Instructions OFFICIAL-SENSITIVE	Example Handling Controls for OFFICIAL-SENSITIVE (not exhaustive)
Access	As business requires	Restricted to those with a right of access	Periodically check access is appropriate
Share with 3rd Party	Allowed	Sharing Agreement in place and secure transfer	Comply with agreement and transfer securely
Take out of workplace	Allowed	Requires management approval	Keep on person when travelling
Clear Desk	Not required	Required and material locked away	Lock papers and equipment away when not in use
Discuss on phone	Allowed	Not in public areas, be aware of surroundings and limit exposure if required	Don’t mention client names
Print	Allowed	Minimum copies necessary, use secure printing, robust handling controls, secure storage and access limited on need to know basis	Always check have all sheets before moving away
Scan	Allowed	Minimum copies necessary, robust handling controls, secure storage and access limited on need to know basis	Don’t copy if not needed
Photocopy	Allowed	Minimum copies necessary, robust handling controls, secure storage and access limited on need to know basis	Don’t copy if not needed
Fax	Allowed	Default position is not permitted. Where requirement for part of operational process this must be fully justified and	Phone, text, email recipient to ensure they have received

		backed up by a risk assessment and user training which includes contacting recipient to ensure receipt – every time	
Post (external)	Allowed	Named recipient. Risk assessment to ascertain if special delivery, courier or hand delivery required	
Post (Internal)	Allowed	Named recipient, hand delivered or sealed envelope	
E-mail (external)	Allowed	Robust checking of named recipients. Sending via secured transport such as SEB (public sector), NHS Interconnect, Clearswift [ENC] or explicit controlled sharing from secure repository	Include identifier in subject heading [OFFICIAL-SENSITIVE] and choose 'Official-Sensitive' label when prompted
E-mail (internal)	Allowed	Robust checking of named recipients (check and double check recipients before hitting send)	Include identifier in subject heading [OFFICIAL-SENSITIVE] and choose 'Official-Sensitive' label when prompted
Misc Electronic Transfer	Allowed	Only after risk assessment and robust process in place	Ensure transfers are encrypted
Make Publicly Available e.g. via Internet	Allowed	Not permitted	
Share using M365 tools e.g. Teams, SharePoint	Allowed	Not permitted (keep checking back for updates)	Use private channels for internal sharing
Council Laptop	Encryption	Encryption	Switch off when not in use, keep in boot of car and take into property overnight
Council owned removable media e.g. CD, Memory stick, USB device	Encryption	Encryption	
Archive	Allowed	Restricted access	User controlled access must remain

System & database testing or development	Allowed	Not Permitted (Real data not permitted within test / development systems)	Data must be anonymised
Destroy (Paper)	Recycle	Shred din level 3 minimum, pulp or burn. Use Council provided confidential waste bins and ensuring key for bins is held securely.	If shredding at home, must use a cross cut shredder
Destroy (Electronic media)	Certified total destruction	Certified total destruction	Pass to ICT for destruction
Loss or Theft	Notify line manager	Notify Line Manager. Notify DPO within 3 hours. If involves ICT equipment or peripherals provide ISO via HW Compromised Form.	Complete form for ISO to ensure risk is addressed
Working in shared open plan office	Allowed	Restricted	Ensure secured from others
Working in public areas	Allowed	Not Permitted	
Personal owned home equipment or other non-Council managed equipment i.e. internet cafe	Allowed	Not Permitted	Not permitted to reside on non-Council managed equipment
Personal owned removable media (e.g.; CD, Memory stick, USB device)	Allowed	Not Permitted	Not permitted to reside on personal removable media of any kind
Personal owned email system	Allowed	Not Permitted	Not permitted to reside within personal email accounts e.g. Hotmail etc.
Vacating Premises	Normal methods of transport acceptable	Information should be checked prior to vacating to ascertain if can be securely destroyed rather than being moved Steps must be taken to ensure: • all paper assets are located, i.e. every drawer and all areas where paper could be trapped is check i.e. behind drawers	Always ensure nothing is left behind – check behind furnishings etc.

		• secure transfer of paper information assets between sites (may include lock boxes, paper accompanied at all times, log of what left and what arrived, etc.). • individuals are identified as having responsibility for all paper asset movement	

CLASSIFICATION OVERVIEW

Classification	Definition
OFFICIAL	Routine business operations information. Information that must be handled in line with instructions but does not require special handling controls and is below the threshold for OFFICIAL-SENSITIVE. Access is mainly restricted to staff and partners (i.e. not the general public). Not published pro-actively or released in an uncontrolled or out of context manner. Could be issued in response to a Freedom of Information request.
OFFICIAL-SENSITIVE	Business sensitive information, personal or special category data under DPA 2018 (GDPR). Information that must be handled in line with instructions and requires special handling controls. Shared on a need to know/named basis. Unauthorised disclosure would cause harm to the Council, other parties or individuals.
NOT OFFICIAL	Information that does not relate to council business or day to day operations. No handling instructions or special handling controls required.

DEFINITIONS

Terminology	Definition
Access	Where a person can physically touch information, can view it even from a distance for example through a window on from a laptop screen, or overhear it when spoken.
Allowed	No special instructions, normal office guidelines and duty of care apply.
Archive	Paper or electronic files that are retained past their operationally active date usually stored because of legal or posterity reasons. Often storage is in authorised archived sites but is sometimes just a spare area in the office.
Business Need	The individuals who can view the information or with whom it is being shared require it in order to provide a service.
Certified Total Destruction	ICT Services use a specialist company to ensure that electronic data is destroyed to the extent that recovery is impossible and they receive a certificate confirming when this is done. Anyone seeking destruction of electronic media should contact the ICT Service Desk.
Clear Desk	Put documents in a drawer or filing cabinet so they are out of sight when you are not at your desk so visitors or staff with no business need to see it would not be able to view the content in passing. Requires to be locked away at end of day.
Courier or Hand Deliver	Don’t use the normal postal system (internal or external) instead arrange a Courier (or use Royal Mail Recorded Delivery) or have a member of staff deliver it in person.
Confirm number & receipt	Check the fax number before pressing send, notify someone at the other end before you send it and confirm they will be waiting at the other end to pick it up. You must ask them to let you know if they do or do not receive it.
Destroy (paper)	See shred
Destroy (electronic)	See Certified Total Destruction for destruction of a device. Using the ‘delete’ button to delete a file from a PC or laptop is acceptable providing that device is sent for Certified Total Destruction when it reaches end of life. Information must not be stored on media which cannot be encrypted.
Discuss on phone	Having a verbal discussion with another party including conference calls
Email (external)	Refers to council email being sent to a non council address
Email (internal)	Refers to ERC council to ERC council email addresses, including schools
Encryption	The councils approved encryption software must be installed and activated. If in doubt, contact the ICT Service Desk for advice.

Terminology	Definition
Escalate if necessary	If a line manager is not around, then escalate to the next most senior person available rather than waiting.
Freedom of Information	Gives individuals the right to ask any public sector organisation for information they hold. Anyone can ask for information.
SEB or file encryption	SEB is a government security standard for ensuring protection of email content in transit across the Internet. Email to other .gov.uk accounts are secured using SEB and therefore emailing from east Renfrewshire email account is accepted. Not everyone has access to SEB protected mail systems and some private sector and third sector companies may not have this security therefore encrypting a file may be the only other option.
ClearSwift [ENC]	Clearswift is a dedicated secured email service provided to allow staff to communicate safely with other parties. Adding [ENC] to the subject line activates security.
Laptop	Refers to council provided laptops used by council staff.
Locked away	Held in a drawer or filing cabinet for example where only those persons authorised to access it have the key or combination to unlock it.
Loss or Theft	Refers to information that has gone missing for any reason.
Minimum copies	Make the absolute minimum copies required and no more. Do not take copies ‘just in case’.
Misc Electronic Transfer	Generally something ICT staff use for bulk data transfers such as FTP/SFTP
Named recipient	You must send to a named individual rather than a generic address or ‘to whom it may concern’ type addresses.
Not Permitted	It is not permitted and the ‘just this once’ or ‘in my judgement’ excuses are not acceptable. If the activity has been granted a formal exception, you will be notified by your manager what alternative measures to use.
None	There are no special instructions, normal office guidelines and duty of care apply.
Notify line manager	Usually required within 2 – 3 hours, if your line manager isn’t available, then escalate by reporting to the next most senior person available.
Open Plan (or shared) Office	An internal council office environment where ERC staff primarily work (with possible exception of the occasional visitor or supplier) but where council staff are not necessarily all from the same Department, Section or Team.
Post (external)	Refers to public mail services such as Royal Mail.
Post (internal)	Refers to using the internal mail system as delivered by Council Officers.
Public area	An environment where members of the public or non Council staff are regularly and freely roaming, where you should have no expectation of privacy or security and have no control over who is in the vicinity. This can include customer facing serving areas, some interview rooms or more obviously when in the street, on a train, in a coffee shop etc. The expectation is you would move to a room where you can control who can hear your conversation and that it is only those directly involved such as a room where no windows are open to a public walkway, doors leading to corridors are closed or people are prevented from passing through or hang about. It does not have to be a council owned room and will often be dedicated meeting or interview room or a managers office. Managers who identify staff with no choice but to remain in a public area, should contact the ISO for advice.
Recycle	Most council offices have a paper recycle bin available.
Removable Media	Devices which are designed to be carried with you or easily sent to another person such as CDRom, memory sticks, external hard drives and SD cards.
Requires management approval	You must obtain permission from your Line Manager first.

Terminology	Definition
Restricted Access	In the office this can mean storing in a cabinet within a secure office and behind access-controlled doors. For archived material it may mean in a secured container inside a zone that requires some form of access control e.g., keypad. The aim is to prevent even colleagues from viewing the material (unless they have their own approved business need).
Sealed envelope	The document must be in an envelope that has been sealed, for internal mail this sealed envelope can then be inserted into an internal mail envelope.
Secured Option	Discuss options with the Information Security Officer to ensure the method chosen is adequately secured.
Share	Providing another non council party such as police or NHS with information collected by council staff. This may occur on a regular or adhoc basis.
Sharing Agreement	This means it is allowed, but only if there is a sharing agreement. The only exception is where the reason is because there is a statutory obligation or, it is based on risk to life and limb and a risk assessment is made beforehand by an appropriate professional e.g., A teacher or social worker believes they have an at risk child in class. After discussion the Head Teacher agrees there may be risk of damage to the child so they will share this information with social workers and police. Sharing agreements are usually written by the Agency that owns the information being shared, in some cases it may be a joint responsibility e.g., if a non ERC organisation is provided with ERC Council information, then ERC generate the Agreement and the other organisation must agree to abide by its conditions. Similarly, if another organisation such as the NHS are providing ERC with the information then they would expect ERC staff to comply with their Agreement. If instructions from another Agency conflict with those of ERC, raise it with your line manager and if necessary, get advice from the ISO.
Shred	Many offices have a shredder which staff can use, some will have secure bins or bags where the documents are taken collectively on a scheduled basis for destruction by an approved organisation. If using such bags, care must be taken to ensure that paperwork cannot accidentally fall out and they must be located in a secured area not accessible to members of the public or visitors.
System & database testing or development	Only ICT staff will be involved with this and it is usually associated with the creation of a new IT application.
Take out of workplace	Information that is removed from the authorised working environment.
Personal owned Home PC	As personal PC's do not meet Data Protection or GDPR standards staff working on PROTECT material would be committing a criminal offence. Staff who have a VDI remote account for home working are allowed to use personal PC's.
Personal owned	Equipment such as computers, laptops, smartphones, tablets, usb storage devices etc. that are not under the control of East Renfrewshire Council
Service DPO	Nominated and trained individual who oversees DPO duties for their own department including investigations into suspected breaches and handling of Subject Access Requests.
HW Compromised Form	Form for lost or stolen hardware or peripherals that have a data bearing ability.