INSPIRING WORLD-CLASS
TEACHING PROFESSIONALISM

Information Security Policy

January 2022

Contact:
Jennifer Macdonald – Director of Regulation and Legal Services and Data Protection Officer

Change control

Version	*Date*	*Detail*
1	14 May 2018	Amendments made to incorporate GDPR
2	March 2021	Review
3	December 2021	Review and rewrite of policy. Amendments made to include remote working, and data integrity, and to refresh the network and application security aspects of the document .

Contents

1.0 Introduction

1.1 Purpose and scope

The confidentiality, integrity and availability of information, in all its forms, is critical to the efficient and effective operation and governance of GTC Scotland[1]. Information is one of our most valuable assets and it is essential that we have adequate safeguards to ensure that it is not lost or compromised.

The purpose of this Policy is to ensure that the GTC Scotland can continue to use personal data to carry out its functions and deliver its services, whilst preventing, or minimising, the impact of information security incidents in relation to personal data. This Policy will assist GTC Scotland in meeting the requirements of Data Protection Law. All users of information being processed by GTC Scotland as a data controller must comply with this Policy. Any failure to comply may result in disciplinary action. All Directors, Managers and individuals will take steps to ensure compliance. The Data Protection Officer (DPO) will ensure that regular audits are undertaken to assess compliance, identify gaps and risks, with appropriate follow-up action to be taken.

All staff will receive appropriate training / briefings in accordance with the information handled within their job role. This Policy will be communicated to all staff during their induction and will be accessible on the GTC Scotland intranet in the Employee Handbook.

This Policy sets down the guiding principles and allocates responsibilities for safeguarding the security of GTC Scotland information. Our guiding principles are:

- Information must be protected from unauthorised access.
- The integrity of our information must be maintained.
- Confidentiality of information (where required) must be assured.
- Regulatory and legislative requirements must be met.
- Information security training must be provided regularly to users to ensure appropriate awareness.
- All breaches of information security (actual or suspected) must be appropriately reported and investigated.

This Policy applies to all GTC Scotland information, systems, networks, applications, locations and the users of them. The term “users” is used throughout this Policy and encompasses all those that use our information within GTC Scotland - this includes staff as well as Council/Panel members and our contractors/consultants and whether they are accessing information from the GTC Scotland office or remotely.

This Policy will be reviewed periodically as part of GTC Scotland’s arrangements for risk management and information security.

[1] GTCS is a public authority with obligations under the Freedom of Information (Scotland) Act 2002 (FOISA) and must also comply with the Public Records (Scotland) Act 2011 (PRSA). In addition, we have a requirement to respect intellectual property law (for example copyright). All of this legislation is relevant to our Information Security Policy and associated procedures.

1.2 Aim

The aim of GTC Scotland's Information Security Policy is to preserve:

1. **Confidentiality:** Confidentiality in the context of this policy means that the data is kept confidential. When information is kept confidential it means that it is not disclosed to people who do not require it or who should not have access to it. Ensuring confidentiality means that information is organised in terms of who needs to have access to it, as well as in terms of its sensitivity. A breach of confidentiality may take place through different means, for instance hacking or unauthorised disclosure.

2. **Integrity:** Data integrity refers to the overall accuracy, completeness and consistency of data. It is maintained by a collection of processes and rules which ensure data is submitted, created, stored and used uniformly. These processes contain rules in relation to the addition, change and deletion of data and include constraints to eliminate duplication of data and to control format, type and amount of data.

3. **Availability:** Availability means that the information is available to users when it is needed. For a system to demonstrate availability, it must have properly functioning computing systems, security controls and communication channels. These systems must be resilient against cyber threats, and have safeguards against power outages, hardware failures and other events that might impact the availability of information.

1.3 Objectives

Our objectives in order to achieve the aim outlined in 1.2 are to:

- Provide a framework for establishing industry-recognised appropriate levels of information security for our information.

- Make sure users are aware of and comply with this Policy, that they understand their information security responsibilities and that we create an information security culture.

- Provide a safe, secure and well-resourced information working environment for users.

- Protect GTC Scotland from liability or damage through the potential misuse of its IT facilities and information systems.

- Undertake a cycle of continuous improvement, responding to feedback and updating our information security arrangements as appropriate.

1.4 Legal context

GTC Scotland is a data controller with obligations set out by law.[2] The law requires us to comply with the following seven data protection principles:

[2] by Data Protecgtion law in the EU General Data Protection Regulation (EU2016/679) ("GDPR"), the Data Protection Act 2018 and other law relating to data protection and the processing of personal data, ("Data Protection Law".

1. Personal data must be processed lawfully, fairly and in a transparent manner;
2. Personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (purpose limitation);
3. Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (data minimisation);
4. Personal data must be accurate and, where necessary, kept up to date (accuracy);
5. Personal data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed (storage limitation);
6. Personal data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (integrity and confidentiality - security).
7. GTC Scotland will be responsible for, and be able to demonstrate, compliance with the data protection principles (accountability).

GTC Scotland must not transfer personal data to another country without appropriate safeguards being put in place and must comply with the rights of data subjects under Data Protection Law, including assisting them in exercising individual rights in relation to their own personal data.

This Policy should be read in conjunction with our Data Protection Policy, in order to understand how we comply with Data Protection law.

1.5 Information classification

We use three information classifications in this Policy:

- **Personal data:** data which relates to a living person who can be identified from that data (or can be identified from that data in combination with other information that is available to us). This mirrors the definition set out in Data Protection Law and includes any expression of opinion about the individual, or of intentions towards him/her. Examples include; staff personnel files, fitness to teach case information and a registered teacher's personal details (e.g. date of birth, national insurance number, payment card data and e-mail address).

- **Controlled Information:** information that we hold that has not been published and we would have to consider carefully before sharing with others (or it may only be appropriate for a restricted group of individuals to view it) as it is potentially sensitive. For example, draft reports, Leadership Team meeting papers or Council papers that have been considered in private.

- **Public Information**: Information that has been published or which we would readily release if a Freedom of Information Act (Scotland) 2002 FOISA request was made for it. For example, information on our website and statistical information.

We need to take the greatest level of care in relation to our use of personal and controlled information – users of this information must ensure that they keep it appropriately safe and secure at all times.

1.6 Related policies and guidance/procedures

There are a number of policies and guidance/procedures related to this Policy and this Policy should be read in conjunction with them; the most significant are listed below.

- Staff Disciplinary Procedure
- Staff Social Media Policy
- Records Management Plan and PolicyRecords Management and Retention ScheduleFlexible Working Policy
- Business Continuity Plan

2.0 Responsibilities2.1 Specific responsibilities

The Extended Leadership Team (ELT) as a whole, led by the Chief Executive, recognises the critical importance of information security to the organisation and will ensure that this Policy is implemented corporately and is monitored. Specific responsibilities of individual members of the organisation are highlighted in the table below.

Role	Responsibility
Director of Regulation and Legal Services (designated as Data Protection Officer)	Responsible for developing this policy as well as ensuring implementation of it across GTC Scotland in order to ensure organisational legal and regulatory compliance.
Senior Manager Digital Services	Responsible for ensuring that the GTC Scotland ICT infrastructure is compliant with the requirements of this policy and that IT processes, including with regards to business continuity, comply with this policy.
Senior Manager Data and Improvement	Responsible for ensuring that the appropriate controls are in place to help protect the integrity of the data held in digital format by GTC Scotland and monitoring GTC Scotland business processes for compliance with the requirements of this policy.
Information Compliance Officer	Responsible for assisting GTC Scotland in meeting its statutory obligations under information compliance legislation including data protection and records management covering both physical and electronic information
All Managers	Managers are responsible working within the requirements of this policy to protect the confidentiality and integrity of the data held by GTC Scotland; ensuring their business processes are compliant with the requirements of this policy; and ensuring that members of their team are: • aware of this Policy • refer this Policy on a regular basis • understand this Policy and its importance to the organisation and comply with it on an ongoing basis in their work (and with regards to the information that they are responsible for processing). Managers must act on any information security instructions provided by the ELT. Managers are expected to ensure that compliance with this Policy features regularly in discussions with

	their staff and in their teams as part of contributing to the development of an information security culture. Managers are also required to support the investigation and management of any suspected data breach.
All Users	All users have a responsibility to comply with this Policy and to keep our information safe and secure. This includes a requirement to report appropriately any suspected data breach (see section 2.4 below). Employees will be provided with regular, mandatory information security training and will be required to confirm annually that they have read this policy

2.2 Compliance and data incidents

It is vital that all users comply with this Policy. Any breach of information security is a serious matter and could lead to the loss of confidentiality, integrity or availability of personal or controlled information. Such a loss may impact our ability to carry out our work and could be both embarrassing and damaging to our reputation. It could also lead to legal or regulatory action against GTCS, including heavy financial penalties.

Any actual or suspected breach of this policy (a data incident) must be notified to the Information Compliance Officer at the earliest possible opportunity and in line with the data incident procedure set out in Annex A. GTC Scotland must ensure that when a possible data incident occurs that a process is followed to ensure that any risk identified is mitigated and the effect of the incident on data subjects is minimal. All employees are encouraged to contact the Information Compliance Officer if they think that a data incident has occurred. All reported data incidents will be investigated and reported to the Leadership Team

Any breach of this policy by a member of staff may be a disciplinary matter and be subject to the disciplinary procedures. Any misuse amounting to criminal conduct will be reported to the police. Where misuse identified severely impacts on system performance or our information security, our Technical Support Team Support will immediately suspend or restrict the user's access privileges.GTC Scotland will ensure appropriate technical and organisational measures are in place to mitigate information security risks associated with remote and mobile working. GTC Scotland will promote an environment in which information security practices are applied appropriately, consistently and logically across all remote and mobile information handling situations to reduce information-related risk to an acceptable level. Users will take responsibility for ensuring the security of the information they handle remotely via a portable device or from non-GTC Scotland managed premises, in line with the GTC Scotland's requirements.

Information should be retained in line with the retention period set down in the Records Management and Retention Schedule which can be found here. http://thehub/fitness-to-teach/RecordManagementandRetention/Records%20Management%20and%20Retention%20Schedule/2021-04-20-RMRS-April-2021.xlsx Personal information must be used only for the purpose it was gathered and must be securely destroyed when it is no longer required for that purpose.

Compliance with this policy is required not only of GTCS staff but also of all our external contractors and Panel/Council members (i.e. all users). The policy is reflected in our standard terms and conditions for contractors and is included in the terms of appointment (or similar) that are set for Panel/Council members.

3.0 Working Practices

3.1 GTC Scotland premises

3.1.1 GTCS operates a clear desk policy at its office premises – you should only have personal or controlled information on your desk when you are using it and are at your desk – you should ensure it is securely stored away at all other times. All records must be stored electronically and any documents received in a paper format, scanned and saved on the Hub. Waste paper must be securely destroyed.

3.1.2 GTC Scotland premises are subject to access controls (or are appropriately locked) to prevent unauthorised access and keep the information that we hold safe and secure. Staff should remain mindful of why these controls are in place and ensure that they are maintained at all times (e.g. the doors should not be propped or wedged open).

3.1.3 Procedures are in place to help staff easily distinguish between employees and visitors. All visitors must be issued with a 'Visitor' badge (that must be worn at all times) when moving around the building and are subject to strict sign-in and sign-out procedures. Some Visitor Badges provide wider access to the office for supplier use – for example those who require access the server room. These are clearly labelled and not issued without authorisation from the appropriate Senior Manager.

3.1.4 Visitors should be accommodated in public meeting rooms as far as possible. Where it is necessary for a visitor to move through any staff office, he/she must be escorted at all times by an employee because personal and controlled information is held in these areas and it is important that this is not accessed in any way (including via overheard conversations).

3.1.5 Where personal or controlled information is held in a physical format, it is important that this isretained in our secure cabinets or our safe. The keys for cabinets must be kept secure in a key safe (to which only authorised staff can access). This should only happen in exceptional circumstances as physical format information is a high security risk. Personal and controlled information should therefore not be taken out of the office in a physical format except where approval has been obtained to do so (at senior management level or above) and it is kept secure at all times.

3.2 Remote and mobile working

3.2.1 GTC Scotland employees are supported to work wherever it is safe and practical do so and to the extent their job and area of work allows. Remote working comprises working on digital or hard copy GTC Scotland information on the move or off-site in a location such as at home. 3.2.2 When working remotely or on the move users must ensure that GTC Scotland Information is handled in accordance with this policy, as applicable to the environment in which they are working.

3.2.3 At all times users should guard against the possibility of unauthorised access to personal and controlled information. Specifically:

- Do not work on or discuss controlled or personal information when connected to free Wifi services offered in public places. These networks may not be secure and could compromise the security of the information. By way of example, it is not appropriate to access and process controlled or personal information related to a fitness to teach case in a public place (e.g. a café or on public transport) but it would be acceptable to work on presentation slides or materials for a training event that are not confidential.

- Controlled or personal information should be in electronic format only to maintain security. Controlled or personal information should never be printed at home as it is not possible to ensure that this is securely destroyed.

- Take steps to ensure that the environment offers a suitable level of privacy (e.g. from other individuals in the vicinity being able to view papers or screens being worked on, or being able to overhear private conversations) before working on controlled or personal information.

- Ensure any paperwork containing controlled or personal information is never left unattended or anywhere it could be misplaced or stolen. This includes being left in an unattended vehicle. Never leave papers or equipment containing controlled or personal information unattended unless they are appropriately physically secured from theft.

- Ensure that your home is kept secure whilst you are working.

- Take precautions when using public or free wi-fi services (such as those commonly found in public libraries and coffee shops) to ensure that any sites to which they are directed are the genuine sites and, once browsing is finished, to log off any services and tell the device to forget the network.

- Do not transmit controlled or personal information (including sending username and password) over an insecure network (e.g. one that does not start with 'https').

3.3 Communication and transfer of information

3.3.1 Users should not send any personal or controlled information by e-mail to an external address unless it is encrypted or otherwise similarly protected. The Digital Services team can be contacted for support and advice by those unsure how to do this. Similarly, users should not send personal or controlled information to their own personal e-mail addresses.,

3.3.2 Users should not save personal or controlled information to another media source (DVD, CD, USB (or memory) key).

3.3.3 Users will ensure that the use of any file transfer, synchronisation and sharing tool to support remote or mobile working is compliant with this policy. The currently approved GTC Scotland file sharing tools are Microsoft SharePoint Online and OneDrive. Industry standard secure transfer tools such as DropBox, WeTransfer, Egress are also acceptable. Users should liaise with the Technical Support Team if they require guidance or support in using SharePoint Online or OneDrive.

3.3.4 Users will ensure they verify the authenticity of callers with verification checks when a registrant (or any other individual) contacts GTC Scotland by telephone and requests information which is deemed to be personal information. Users must be able to confirm that the person contacting is the registrant or person entitled to receive the personal information. Particular caution must be exercised if asked to provide personal information over the telephone. Appropriate verification (or security) checks must be followed. The minimum checks which should be established are GTC Scotland name, registration number, date of birth and postcode.

3.3.5 E-mail and address details must be treated with similar caution until they have been confirmed. Staff must err on the side of caution when a request to provide personal information is received and seek advice from the Information Compliance Officer as required.

3.3.7 Where there is a requirement to transfer or transmit personal or controlled information in a physical form, this must be done in a secure way. Where postal or courier services are used, the information should be packaged up in an appropriately strong and durable envelope (or equivalent) to mitigate damage in transit.

4.0 User Management

4.1 Network access controls

4.1.1 Users must use secure remote access methods for accessing GTC Scotland networks when working remotely. The remote access service is the Windows VPN (password controlled). There is also access to e-mails via the Office365 portal and via the online portal for restricted information sharing for Panel/Council members. Users should not attempt to gain access to our networks in any other way.

4.1.2 Access to the GTC Scotland network (and all of our electronically held records and information) is controlled by a user authorisation procedure which is subject to an HR process and approval at senior manager level or above. Access rights are administered by the Digital Services Team and/or the IT Managed Service provider. Users are provided access only to the information or systems that are required to fulfil the role.

4.1.3 When a user leaves GTC Scotland employment (or similar), all of their system log-ons must be immediately revoked and any other access to information via mobile phones, iPads, remote access or in any other way must be immediately removed. Managers are responsible for ensuring that the following events are communicated to the Digital Services team so that the appropriate steps are then taken.

- Leavers (leaving GTC Scotland, including secondments?) – Managers should use the Leavers form (available on The Hub or from HR). Once Digital Services have the required information from Managers (via the Leavers form), they will action the IT off-boarding process.
- Role changers (remaining within GTC Scotland) – Managers should notify Digital Services of any change to access controls for an individual (either increased or reduced) as a result of a role change. Any increased IT permissions should be requested to Digital Services via email by the authorising manager and approved by the Senior Manager Digital Services.

4.1.4 The retention period for existing records of GTC Scotland leavers is 6 months from leaving date.

4.1.5 If, due to an unexpected absence, access to a member of staff's user logon (or similar) is deemed appropriate, then this must be authorised by a Leadership Team member, Senior Manager Digital Services or HR Manager.

4.2 Application access controls

4.2.1 Access to GTC Scotland applications is controlled and restricted to authorised users who have a legitimate business need.

4.2.2 User access to the Register of Teachers database (in Dynamics 365) is controlled by password protected user accounts which are only set up and issued to users by designated members of the Digital Services Team. Access to Dynamics 365 is set only for those members of staff who

require access to teachers' records for work purposes. Levels of access are set according to individual job remits. View only access can be set where applicable. User movements are recorded and can be audited and reported on.

4.2.3 Access to administer the GTC Scotland online payment facility must be authorised by a Senior Manager (or above) and only where this is a business need.

4.3 Password management

4.3.1 All users are issued with a unique username for a password-protected account which must be used only by the named person.

4.3.2 Users must not share their account or password details with any other person or attempt to gain access to any account other than their own unless authorised to do so by a member of LT.

4.3.3 Users are responsible for all activity recorded against their account.

4.3.4 If users need to store their password, they must do so in a way that is hidden or encrypted – consult the Digital Services team for advice on this if needed.

4.3.5 The system requires users to change passwords regularly for cyber security reasons and the following controls are in place to ensure all passwords are sufficiently complex and secure.

- Minimum password length must be at least 12 characters
- Password must include Capital letters, small letters, numbers and symbols.
- Users are required to reset passwords every 90 days
- Users will not be permitted to use passwords previously used
- Users are advised not to use common phrases, dates or words from the dictionary

4.3.6 For those who act as IT system administrators, all IT admin passwords/users should have two-factor authentication enabled as a minimum. All two-factor authentication should be removed from mobile devices when a user leaves GTC Scotland.

4.3.7 All passwords should be audited through use of ethical hacking annually to ensure compliance on user and admin accounts and to update best practice as it evolves.

5.0 Security

5.1 Security controls

GTC Scotland has the following security controls implemented within the IT infrastructure:

- Data Loss Prevention – Office 365 policies
- Email Filtering – Office 365
- Intrusion Detection System – Sonicwall Firewall
- Perimeter Firewalls – Sonicwall Firewall

- Web Content Filtering – GFI Proxy solution
- Asset Inventory – Lansweeper tool
- DDoS Mitigation – Sonicwall Firewall
- Security Info & Event management – ElasticSearch
- DMARC – Office 365/DNS
- Endpoint protection – McAfee AV
- Penetration testing – Third party (Commissum)
- Web Application Firewall – Microsoft WAP solution

5.2 Server Patch Management

5.2.1 All servers are patched on a monthly, ongoing basis by the IT Managed Service Provider. Patching must be authorised each month by the Senior Manager Digital Services before it takes place.

5.3 Infrastructure Vulnerability Testing

5.3.1 External penetration testing is organised on an annual basis and is conducted by external contractors on external facing IP addresses. A report is provided showing the findings and recommendations arising from the testing. Action is taken as required on reported findings to ensure we continue to maintain best practice in the security of our information and it is not at risk.

5.3.2 Web Application security testing is performed after changes have been applied to our applications. Given the cycle of continual updates across most of our applications, we schedule this on an annual basis. A report is provided showing the findings and recommendations arising from the testing. Action is taken as required on reported findings.

This testing currently covers the following applications:

- Dynamics 365 (including the Register of Teachers)
- MyGTCS
- MyPL system
- Teacher Inducation Scheme Profile System
- Flexible Route Profile System
- ITE Profile System
- Student Placement System
- www.gtcs,org.uk website
- Online applications via Dynamics portals
- Flexible Route Virtual School

5.3.3 Quarterly ASV (Approved Scanning Vendor) scans are performed to ensure our systems are of a security level to meet the standards of PCI compliance. Reports on each relevant IP address are provided showing the findings and recommendations arising from the testing. Action is taken as required on reported findings.

5.4 Virus prevention

5.4.1 Laptop equipment and server equipment, along with any other endpoint device that requires it, has been pre-installed with antivirus software. However, antivirus software will not protect systems (and by implication connected systems) against viruses unless it is continuously kept

up to date with the latest known virus profiles. The Digital Services function and the IT Managed Service Provider are responsible for ensuring this process takes place.

5.4.2 GTC Scotland uses Office 365 Advanced Threat Protection within Outlook to protect mailboxes against new, sophisticated malware attacks via unsafe attachments and malicious links

5.4.3 To help prevent the spread of computer viruses, users must observe the following simple precautions:

- Only download files which you are certain are genuine. Exercise particular caution when opening e-mail attachments, especially unsolicited communications, as this route may transmit viruses. Any files downloaded from e-mail received from a non-GTCS source must be scanned by GTC Scotland's detection software. When in doubt view the attachment first and only open it if you recognise the contents of the message. Microsoft Word files are especially prone to virus attack.

- Do not bring any private external storage devices into the office for use on the GTC Scotland network unless by agreement with Technical Support who will virus check the device.

5.4.4 Any suspicion that a virus may have entered the system must be reported immediately to the Digital Services team who will report it to the IT Managed Service Provider. Consideration will then be given to whether there is a potential data incident to be reported in accordance with Annex A.

5.5 Back-up procedures

5.5.1 Datacentre servers are backed up on a nightly basis. Data held on the VIIA platform (in Clerwood House or NVT Datacentre) is backed up each night (Monday to Friday). The backups Monday to Thursday are incremental backups (changes) and the Friday backup is a full backup. These backups go offsite to a tertiary datacentre.

5.5.2 The Clerwood House servers are currently backed up each night to disk storage, and this storage sits within the same server room/building as the live equipment. These servers will be removed from the infrastructure once the services running on them (The Hub, Miller and Business Objects) are decommissioned (early 2022).

5.6 Hardware (laptops, tablets and mobile devices)

5.6.1 All GTC Scotland employees are issued with laptops and some employees are issued with tablets or mobile phones (if required for their role). All hardware remains the property of GTC Scotland. Council/panel members and contractors are not issued with hardware by GTC Scotland.

5.6.2 All IT hardware assets must be recorded in Lansweeper by a member of the Digital Services team and recorded against the individual to which they are assigned. This should be audited routinely for replacement schedule and to make sure it remains current and up to date. This should also include the software which includes anti-virus on the devices to be patched and kept up to date.

5.6.3 GTC Scotland equipment must be kept secure at all times and should only be accessible to other GTC Scotland users.

5.6.4 GTC Scotland hardware must not be used by, given or loaned to anyone who does not work for GTC Scotland. This includes family members at home where an individual is working remotely.

5.6.5 GTC Scotland hardware must be stored safely and securely, for example in the locked boot of a car rather than on a seat.

5.6.6 All devices must be encrypted so that in the event of a loss or theft, data cannot be recovered if found by an unauthorised person. The Digital Services team and the IT Managed Service provider have responsibility for ensuring this is done. This will be routinely audited through the Cyber Essential accreditation programme to ensure compliance.

5.6.7 All laptops are set to automatically lock after 10 minutes of inactivity.

5.6.8 Users must take reasonable care of GTC Scotland hardware and protect it from physical damage wherever possible, ie:

- Take reasonable and common-sense precautions to avoid drinks or liquids being spilled on hardware.
- Always carry hardware in any protective bags or boxes provided.
- Do not place hardware on furniture that is not designed to support it.

5.6.9 Users should not use their own devices to access the GTC Scotland network as a general rule. We allow Panel/Council members to access our information sharing portal via their own devices. This portal is subject to secure log-in and password controls and members are prohibited from downloading or storing to their own devices (or other personal storage facilities) copies of the information provided. Staff may access Microsoft Office 365 (Outlook software – e-mail) on their own devices but should do so as an exception, where this is required.

5.6.10 Employees must ensure they return all hardware to the Digital Services team before leaving the organisation, in line with the HR Leavers process.

5.6.11 Loss of any hardware is a data incident and should be reported using the procedure set out in Annex A. Loss of equipment (including cables, cases, batteries and any other peripherals provided) due to a lack of reasonable care and adherence to this policy my result in disciplinary action.

5.7 Secure destruction and disposal

5.7.1 All unused 'Data Bearing Devices' (i.e. computer hardware) will be removed and securely destroyed by a certified contractor guaranteeing 100% secure physical destruction. A Certificate of Secure Data Destruction is issued by the contractor carrying out the work. Any secure disposal of IT equipment must be arranged by the Digital Services function.

5.7.2 All information held in a physical format (e.g. paper, disc or tape) is subject to similar, secure shredding using our preferred supplier). A Certificate of Secure Data Destruction is issued by the contractor carrying out the work. Information is held in a secure, locked location pending destruction (and may only be accessed with the approval (and under the strict supervision) of a Manager).

5.7.3 Users should never print documentation that contains controlled or personal information at home. Any hard copy documentation containing controlled or personal information must be destroyed securely such as being deposited in confidential waste bins or shredded, and as this is not possible at home, printing documents containing controlled or personal information at home is deemed as breaching the requirements of this policy.

5.7.4 Card holder data will not be stored in the database after payments are made using the GTC Scotland payment facility. Users should not, under any circumstances, store payment card information.

5.8 Email security

5.8.1 GTC Scotland uses appropriate encryption methods via Office 365 Advanced Threat Protection to improve email security.

5.8.2 Email is not an informal communication tool; it has the same authority as any other method of communication. The same laws apply to email as any other written document therefore it is essential to avoid making inaccurate or defamatory statements. Binding contracts may also be inadvertently created, so always exercise due care. If in doubt, seek advice.

5.8.3 All email messages that are created, sent, received or stored on GTC Scotland's email system are the sole property of GTC Scotland. Each employee is responsible for all email sent from his or her e-mail account.

5.8.4 All external emails must have GTC Scotland's standard disclaimer set out in them. This is contained within the auto-signature, the content of which is managed by the Communications and Digital Services teams and must not be changed by the user.

5.8.5 No employee at any level may access the email of another employee without their consent (ie, they have been granted Delegate access), unless specifically authorised to do so by a member of the Extended Leadership Team for business purposes.

5.8.6 Email inboxes should be cleared out regularly in line with our Records Management and Retention Policy. Emails are automatically deleted from all GTC Scotland email accounts after 1 year. Important emails should be saved in the relevant section of The Hub.

5.8.7 Users should always check and verify the recipient's address before sending an email, particularly where the information to be sent is controlled or personal.

5.8.8 Users must not access the Criminal Justice Secure email Service from a device that does not belong to GTC Scotland.

Annex 1 – Data Incident Response Procedure

Any data incident may give rise to a personal data breach, defined in law as "the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed." Examples of data security incidents include:

- Loss or theft of data or equipment on which data is stored
- Deliberate and unauthorised unavailability of a system
- Unauthorised access to a system
- Equipment failure
- Human error
- Unforeseen circumstances such as a fire or flood
- Hacking attack
- Blagging offences where information is obtained by deceit

GTC Scotland's Data Protection Officer (DPO) has overall responsibility within GTC Scotland for ensuring that personal data security risks are assessed and mitigated to an acceptable level. The DPO is supported in this role by the GTC Scotland Information Compliance Officer.

The DPO is responsible for ensuring that GTC Scotland complies with all relevant Data Protection Law by providing for the development, maintenance and auditing of GTC Scotland's information security arrangements. The DPO will ensure that the Extended Leadership Team and the Council of GTC Scotland receive appropriate advice in relation to the identification and mitigation of data protection and information security risks.

The DPO, supported by the Information Compliance Officer, will co-ordinate the investigation of information security incidents and ensure the appropriate recording and reporting of security incidents at local and national level.

Reporting an Information Security Incident

Any person who believes a data incident has or is occurring must inform either their Senior Manager or Director without delay. In all cases, the GTC Scotland Data Incident Form which is available through a link on the Hub must be completed with available information before being submitted to the Information Compliance Officer by email to dataprotection@gcts.org.uk. The report **must** be submitted to the Information Compliance Officer in any event within 24 hours of the incident being discovered.

The Information Compliance Officer will direct any investigation of a data incident. Under normal circumstances, Senior Managers must not conduct investigations prior to any incident being formally reported to the Information Compliance Officer. However, where any delay in the investigation may result in the loss of evidence then the Senior Manager must discuss this with the Information Compliance Officer so that an investigation can begin immediately. All data incidents will be logged on the GTC Scotland Data Incident Log.

Information Incident Management

The Information Compliance Officer will firstly determine if the breach is still occurring. If so, the appropriate steps will be taken immediately to minimise the effect of the breach.

An initial assessment will be made by the Information Compliance Officer in liaison with relevant staff to establish the severity of the breach and who will take the lead investigating the breach (this will depend on the nature of the breach in some cases it could be a member of the Leadership Team).

IT personnel will establish whether there is anything that can be done to recover any losses and limit the damage the breach could cause.

The Information Compliance Officer in liaison with other relevant personnel will determine the suitable course of action to be taken to ensure a resolution to the incident. The Information Compliance Officer is responsible for reporting to incident in full to the Leadership Team.

An investigation will be undertaken by the Information Compliance Officer and wherever possible within 24 hours of the breach being discovered/reported.

The Information Compliance Officer will investigate the breach and assess the risks associated with it, for example, the potential adverse consequences for individuals, how serious or substantial those are and how likely they are to occur.

Data security breaches will require an initial response to investigate and contain the situation as well as a recovery plan including, where necessary, damage limitation. This will often involve input from specialists in IT, HR and legal and in some cases contact with external stakeholders and suppliers. The following actions should be considered:

- Establish who needs to be made aware of the breach and inform them of what they are expected to do to assist in the containment exercise, e.g. this could be isolating or closing a compromised section of the network or finding a lost piece of equipment.

- Establish whether there is anything that can be done to recover any losses and limit the damage the breach can cause. As well as the physical recovery of equipment, this could involve the use of back up tapes to restore lost or damaged data or ensuring that staff recognise when someone tries to use stolen data to access accounts.

- Where appropriate, inform the police, if it is considered that a criminal offence may have been committed.

Notification

The Information Compliance Officer, in conjunction with the Leadership Team where practicable, will determine whether a notification is required and if so, to whom.

Under Article 33 of the UK GDPR, a controller must without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the **ICO**, unless the personal data breach is unlikely to result in a **risk** to the rights and freedoms of natural persons. Where the notification to the ICO is not made within 72 hours, it must be accompanied by reasons for the delay.

Under Article 34 of the UK GDPR, when the personal data breach is likely to result in a **high risk** to the rights and freedoms of natural persons, the controller must communicate the personal data breach to the **data subject** without undue delay. In assessing the level of risk for the purposes of notification, the Information Compliance Officer, in conjunction with the Leadership Team where practicable, will refer, amongst other things, to factors listed in Annex A to this policy.

Where notification is not required

Article 33(1) of the UK GDPR makes it clear that breaches that are “unlikely to result in a risk to the rights and freedoms of natural persons” do not require notification to the supervisory authority. An

example might be where personal data are already publicly available and a disclosure of such data does not constitute a likely risk to the individual.

If personal data have been made essentially unintelligible to unauthorised parties and where the data are a copy or a backup exists, a confidentiality breach involving properly encrypted personal data may not need to be notified to the supervisory authority. This is because such a breach is unlikely to pose a risk to individuals' rights and freedoms.

However, if there is a breach where there are no backups of the encrypted personal data then there will have been an availability breach, which could pose risks to individuals and therefore may require notification.

Where a breach occurs involving the loss of encrypted data, even if a backup of the personal data exists this may still be a reportable breach, depending on the length of time taken to restore the data from that backup and the effect that lack of availability has on individuals

Notification to the ICO

As above, GTC Scotland must notify the UK ICO of any notifiable breach without undue delay and, where feasible, not later than 72 hours after having become aware of it.

GTC Scotland will be regarded as having become "aware" of a breach when it has a reasonable degree of certainty that a security incident has occurred that has led to personal data being compromised. When, exactly, GTC Scotland can be considered to be "aware" of a particular breach will depend on the circumstances of the specific breach. In some cases, it will be relatively clear from the outset that there has been a breach whereas, in others, it may take some.

After first being informed of a potential breach by an individual, a media organisation, or another source, or when it has itself detected a security incident, the GTC Scotland Information Compliance Officer may undertake a short period of investigation in order to establish whether or not a breach has in fact occurred (as detailed above). During this period of investigation, GTC Scotland may not be regarded as being "aware". However, the GDPR requires the controller to implement all appropriate technical protection and organisational measures to establish immediately whether a breach has taken place and to inform promptly the supervisory authority and the data subjects. This puts an obligation on GTC Scotland to ensure that they will be "aware" of any breaches in a timely manner so that they can take appropriate action.

As a minimum, the following information must be provided to the ICO where a notification is required:

- description of the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
- name and contact details of the data protection officer or other contact point where more information can be obtained;
- description of the likely consequences of the personal data breach;
- description of the measures taken or proposed to be taken by the GTC Scotland to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where precise information is not available (e.g. exact number of data subjects affected) this should not be a barrier to timely breach notification. The UK GDPR allows for approximations to be made in the number of individuals affected and the number of personal data records concerned.

Where it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay, with more investigation and follow-up with additional information at a later point. When the GTC Scotland first notifies the ICO, they should also inform the ICO if they do not yet have all the required information and that they will provide more details later on.

Where notification authority is not made within 72 hours, it must be accompanied by reasons for the delay

Notification to the Data Subject

Where there is likely to be a **high risk** to the rights and freedoms of individuals as the result of a breach, individuals must also be informed.

There is no specific time-limit for notifying individuals about a breach, but communications should be made "without undue delay".

As a minimum, the following information should be provided to the individual:

- a description of the nature of the breach;
- the name and contact details of the DPO, or other contact point;
- a description of the likely consequences of the breach; and
- a description of the measures taken or proposed to be taken by the controller to address the breach, including, where appropriate, measures to mitigate its possible adverse effects.

The communication should be made to the affected data subjects directly, unless doing so would involve a disproportionate effort. In such a case, there will instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

Any communication sent to an individual should not be sent with other information, such as regular updates, newsletters, or standard messages.

Prior to contacting the individual, GTC Scotland may wish to consult the ICO to seek advice about an appropriate message and the most appropriate form of contact.

In some specific circumstances, it may not be necessary to contact the individual:

- where GTC Scotland has applied appropriate technical and organisational measures to protect personal data prior to the breach, in particular those measures that render personal data unintelligible to any person who is not authorised to access it. This could, for example, include protecting personal data with state-of-the-art encryption, or by tokenization.
- Immediately following a breach, GTC Scotland has taken steps to ensure that the high risk posed to individuals' rights and freedoms is no longer likely to materialise. For example, depending on the circumstances of the case, GTC Scotland may have immediately identified and taken action against the individual who has accessed personal data before they were able to do anything with it. Due regard still needs to be given to the possible consequences of any breach of confidentiality, again, depending on the nature of the data concerned.
- It would involve disproportionate effort to contact individuals, perhaps where their contact details have been lost as a result of the breach or are not known in the first place. In the case of disproportionate effort, technical arrangements could also be envisaged to make information about the breach available on demand, which could prove useful to those individuals who may be affected by a breach, but the controller cannot otherwise contact.

Additional Notifications

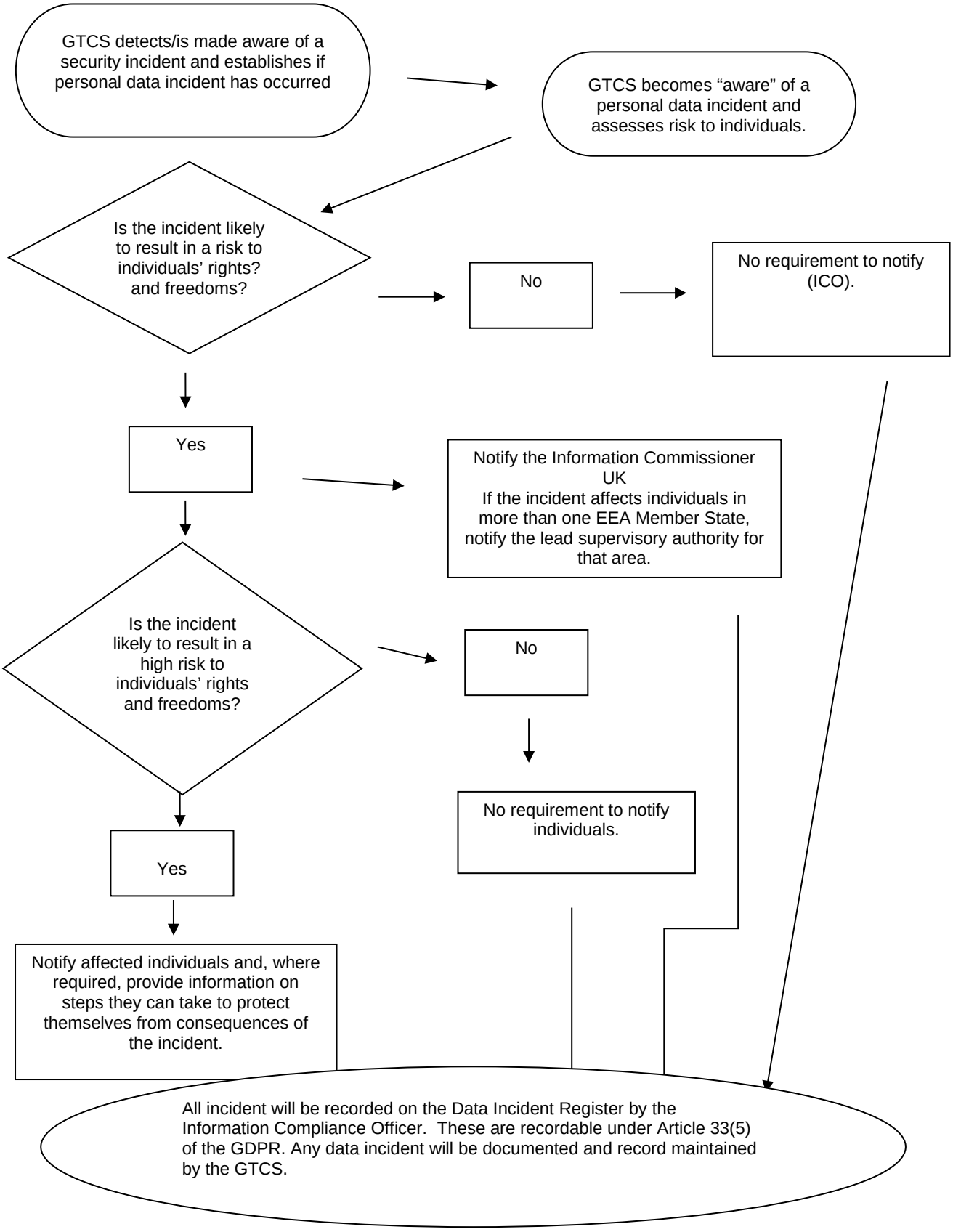
GTC Scotland through the Leadership Team and DPO, must consider notifying third parties such as the police, insurers, bank or credit card companies, and trade unions. This would be appropriate where illegal activity is known or is believed to have occurred, or where there is a risk that illegal activity might occur in the future.

They will also consider whether the GTC Scotland's Communications Manager should be informed, to consider how to handle media enquiries or to consider the terms of a press release.

A report of the incident which has occurred will be reported to the Leadership Team on each occurrence and where necessary will also be reported to external and regulatory bodies

All actions will be recorded by the Information Compliance Officer and regular reporting to the Leadership Team will be undertaken.

GTCS Data Incident Response Procedure - Flowchart of notification requirements



Examples of personal data breaches and who to notify

Example	Notify the supervisory authority?	Notify the data subject?	Notes/recommendations
i. A controller stored a backup of an archive of personal data encrypted on a USB key. The key is stolen during a break-in.	No.	No.	As long as the data are encrypted with a state of the art algorithm, backups of the data exist the unique key is not compromised, and the data can be restored in good time, this may not be a reportable breach. However, if it is later compromised, notification is required.
ii. A controller maintains an online service. As a result of a cyber-attack on that service, personal data of individuals are exfiltrated (transferred out). The controller is processing personal data of individuals in a single Member State.	Yes, report to the supervisory authority if there are likely consequences to individuals.	Yes, report to individuals depending on the nature of the personal data affected and if the severity of the likely consequences to individuals is high.	
iii. A brief power outage lasting several minutes at a controller's call centre meaning individuals are unable to call the controller and access their records.	No.	No.	This is not a notifiable breach, but still a recordable incident under Article 33(5). Appropriate records should be maintained by the controller.
iv. A controller suffers a ransomware attack which results in all data being encrypted. No back-ups are available and the data cannot be restored. On investigation, it becomes clear that the ransomware's only functionality was to encrypt the data, and that there was no other malware present in the system.	Yes, report to the supervisory authority, if there are likely consequences to individuals as this is a loss of availability.	Yes, report to individuals, depending on the nature of the personal data affected and the possible effect of the lack of availability of the data, as well as other likely	If there was a backup available and data could be restored in good time, this would not need to be reported to the supervisory authority or to individuals as there would have been no permanent loss of availability or confidentiality. However, if the supervisory authority became aware of the incident by other means, it may consider an investigation to assess compliance with the broader security requirements of Article 32.

Factors to consider when assessing risk

When assessing risk, consideration should be given to both the **likelihood** and **severity** of the risk to the rights and freedoms of data subjects. The following criteria will be particularly relevant in assessing the risk involved in a data breach:

Type of breach	"Confidentiality breach" - where there is an unauthorised or accidental disclosure of, or access to, personal data. "Integrity breach" - where there is an unauthorised or accidental alteration of personal data. "Availability breach" - where there is an accidental or unauthorised loss of access to, or destruction of, personal data
The nature, sensitivity, and volume of personal data	Usually, the more sensitive the data, the higher the risk of harm will be to the people affected, but consideration should also be given to other personal data that may already be available about the data subject. A combination of personal data is typically more sensitive than a single piece of personal data. Some types of personal data may seem at first relatively innocuous, however, what that data may reveal about the affected individual should be carefully considered e.g. would it facilitate the committal of crimes against them. A small amount of highly sensitive personal data can have a high impact on an individual, and a large range of details can reveal a greater range of information about that individual
Ease of identification of individuals	How easy it will be for a party who has access to compromised personal data to identify specific individuals, or match the data with other information to identify individuals
Severity of consequences for individuals.	Depending on the nature of the personal data involved in a breach, for example, special categories of data, the potential damage to individuals that could result can be especially severe, in particular where the breach could result in identity theft or fraud, physical harm, psychological distress, humiliation or damage to reputation. If the breach concerns personal data about vulnerable individuals, they could be placed at greater risk of harm. Whether the controller is aware that personal data is in the hands of people whose intentions are unknown or possibly malicious can have a bearing on the level of potential risk.

Special characteristics of the individual	A breach may affect personal data concerning children or other vulnerable individuals, who may be placed at greater risk of danger as a result.
Special characteristics of the data controller	The nature and role of the controller and its activities may affect the level of risk to individuals as a result of a breach. For example, certain organisations may routinely process special categories of personal data, meaning that there is a greater threat to individuals if their personal data is breached, compared with a mailing list of a newspaper.
The number of affected individuals	Generally, the higher the number of individuals affected, the greater the impact of a breach can have.

Annex 2 - Payment Card Security Incident Response Plan

If a data breach is suspected which involves credit card data a member of the PCI Response Team must be alerted in addition to following the data breach procedure set out in Annex A.

PCI Response Team:
Senior Manager: Data and Improvement
Senior Manager: Digital Services
Digital Product Manager

1. Each department must report an incident to a member of the PCI Response Team.

2. The PCI Response Team will investigate the incident and assist the potentially compromised department in limiting the exposure of cardholder data and in mitigating the risks associated with the incident.

3. The PCI Response Team will resolve the problem to the satisfaction of all parties involved, including reporting the incident and findings to the appropriate parties (credit card associations, credit card processors, etc) as necessary.

4. The PCI Response Team will determine if policies and processes need to be updated to avoid a similar incident in the future, and whether additional safeguards are required in the environment where the incident occurred, or for the institution.

5. If an unauthorised wireless access point or devices is identified or detected as part of the quarterly test this should be removed immediately.

The card companies have individually specific requirements the Response Team must address in reporting suspected or confirmed breaches of cardholder data. These details are held by the PCI Incident Response Team.