DRIVING FORWARD PROFESSIONAL
STANDARDS FOR TEACHERS

THE GENERAL
TEACHING COUNCIL
FOR SCOTLAND

gtc SCOTLAND

Information Security Policy

May 2018

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

1.0 GENERAL INFORMATION

1.1 Introduction

The confidentiality, integrity and availability of information, in all its forms, is critical to the efficient and effective operation and governance of GTCS[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.

1.2 Purpose and scope

Information is an important asset for GTCS and performing its functions and delivering its services. The purpose of this Policy is to ensure that the GTCS 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 GTCS in meeting the requirements of Data Protection Law. All users of information being processed by GTCS as a data controller must comply with this Policy. Any failure to comply may result in disciplinary action. All Senior Managers and Directors will take steps to ensure compliance. The DPO will ensure that all regular audits are undertaken to assess compliance, identify gaps and risks, with appropriate follow-up action to be taken.

This Policy will be reviewed periodically as part of GTCS's arrangements for risk management and information security. It should be read in conjunction with our Data Protection Policy and relevant sections of GTCS's Records Management Plan and Policy, Staff Disciplinary Procedure, Staff Social Media Policy, Records Management and Retention Schedule and Business Continuity Plan.

All staff will receive appropriate training / briefings according to the information handled within their job role. This Policy will be communicated to all staff via Senior Managers and will be accessible on the GTCS intranet. It will also be included in the GTCS Employee Handbook.

This Policy sets down the guiding principles and allocates responsibilities for safeguarding the security of GTCS 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 all staff to ensure appropriate awareness.
- All breaches of information security (actual or suspected) must be appropriately reported and investigated.

This Policy applies to all GTCS 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 GTCS - this includes staff as well as Council/Panel members and our contractors/consultants.

[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.

1.3 Objectives

Our objectives in order to achieve the guiding principles outline 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 system working environment for users.

- Protect GCTS 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 update as appropriate.

1.4 Legal context

GTCS is a data controller with obligations set out by law.[2] The law requires us to comply with the certain data protection principles, which require that personal data must be:

1. processed lawfully, fairly and in a transparent manner;
2. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
3. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
4. accurate and, where necessary, kept up to date;
5. 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;
6. 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).
7. GTCS will be responsible for, and be able to demonstrate, compliance with the data protection principles (accountability).

GTCS 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.

GTCS will be responsible for, and be able to demonstrate, compliance with the data protection principles, in accordance with the requirement for accountability in GDPR.

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

[2] by Data Protection 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”.

1.5 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, Corporate Management 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 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; the most significant are listed below.

- Staff Disciplinary Procedure
- Staff Social Media Policy
- Records Management Plan and Policy
- Records Management and Retention Schedule
- Business Continuity Plan

2.0 RESPONSIBILITIES

2.1 Corporate Management Team

The Corporate Management Team (CMT) 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 CMT 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 GTCS in order to ensure organisational legal and regulatory compliance.
Director of Corporate Services	Responsible for ensuring that the GTCS ICT infrastructure is compliant with the requirements of this policy and that GTCS

	business processes comply with the requirements of this policy, including as regards business continuity.

2.2 Senior Managers

- Senior Managers are responsible for ensuring that their staff are:
- aware of this Policy
- read 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).

Senior Managers must act on any information security instructions provide by the CMT. Senior 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. Senior Managers are also required to support the investigation and management of any suspected data breach.

2.3 Individuals

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).

Staff will be provided with regular, mandatory information security training and will be required to confirm annually that they have read this policy.

2.4 Compliance, information sharing and data breaches

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.

Users should not send any personal or controlled information by e-mail to an external address unless it is encrypted or otherwise similarly protected. Similarly, users should not send personal or controlled information to their own personal e-mail addresses. Information should be retained in line with the retention period set down in the Records Management and Retention Schedule. 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.

Any actual or suspected breach of this policy must be notified to the Director of Regulation and Legal Services at the earliest possible opportunity and in line with the data breach procedure set out in Annex A. All reported data breaches will be investigated and reported to the Corporate Management 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.

Compliance with this policy is required not only of GTCS staff but also of all our external contractors and Panel/Council members. 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 PHYSICAL SECURITY

3.1 General

- GTCS operates a clear desk policy – 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 waste paper should be securely destroyed.

- Our staff offices 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).

- 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.

- 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).

- Where personal or controlled information is held in a physical format, it is important that this is retained in our secure cabinets or our safe. The keys for cabinets must be kept secure in a key safe (to which other staff can access). Physical format information is a high security risk. Personal and controlled information should therefore not generally 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. To ensure an appropriate audit trail, the physical record sign-out spreadsheet should also be completed where personal or controlled information is being taken out of the office in a physical format.

- Personal information should not be issued to an individual without checking that the individual is entitled to access the information and is genuine. Particular caution should be exercised when providing personal information over the telephone and appropriate verification (or security) checks must be followed. E-mail and address details should be treated with similar caution until they have been confirmed. Staff should err on the side of caution in providing any information and seek advice as required.

- 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.

3.2 Network access control

3.2.1 User management

- Access to the GTCS network (and all of our electronically held records and information) is controlled by a user authorisation procedure. The level of access that is provided (ultimately by our IT Support provider) is controlled through this authorisation procedure which is subject to an HR process and approval at senior manager level or above. Access rights are administered by the Technical Support Team. Users are provided access only to the information or systems that are required to fulfil the role.

- When a user leaves GTCS 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. Senior managers (and above) are responsible for ensuring that such events are communicated to the digital development department so that these steps are then taken.

- 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 CMT member.

- All users are required to agree to the GTCS acceptable use policy as part of the network logon process.

2.2.2 Passwords

- All users are issued with a unique user account name and password which must be used only by the named person.

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

- 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 CMT.

- If you need to store your password, you must do so in a way that is hidden or encrypted – consult the Technical Support Team for advice on this if needed.

- The system requires users to change passwords regularly for information security reasons and best practice has now been provided to all staff and is summarised below:

    - Minimum password length should be at least 12 characters

    - Your password must include Capital letters, small letters, numbers and symbols.

    - You will be required to reset passwords every 90 days

    - You should not use passwords previously used

    - You should not use common phrases, dates or words from the dictionary

3.3 Hardware use (laptops, tablets and mobile devices)

3.3.1 General

- GTCS equipment must be kept secure at all times and should only be accessible to other GTCS users.

- Our hardware must not be used by, given or loaned to anyone who does not work for GTCS.

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

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

- Users should ensure that there is no possibility that confidential or controlled information may be accessed or viewed when using such information. By way of example, it would not be appropriate to access and process personal information related to a fitness to teach case in a public place (e.g. while travelling to work on a train) but it would be fine to work on slides or materials for a training event that are not confidential. Similar precautions should be exercised in terms of printing any documents – the locked print function should be used where appropriate.

- Users should not save personal or controlled information to another media source (DVD, CD, USB (or memory) key). They should only save this information to the GTCS Hub. If there is a need to transfer the information, you should liaise with the Technical Support Team and set up a secure information sharing portal or use the signposted e-mail encryption software.

- Users must take reasonable care of GTCS hardware and protect it from physical damage wherever possible:

  - 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.

- Users should not use their own devices to access the GTCS 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.

- GTCS is responsible for all information stored on our hardware. No personal (non-work related) files should be saved to GTCS equipment - our Microsoft Office suite makes it easy to save any such files to a personal OneDrive. Under no circumstances should files be stored that are covered by copyright (or other intellectual property rights) and we do not have the proper permission to use them.

- Employees must ensure they return all hardware to their line manager before leaving the organisation in line with the HR Leavers process. In other circumstances, if the requirement for equipment changes, surplus equipment should be returned to the Technical Support Team.

- Loss of any hardware constitutes a potential data breach and should be reported to your line manager and using the procedure set out in Annex 1. Loss of equipment due to a lack of reasonable care and adherence to this policy my result in disciplinary action being taken.

3.3.2 Remote access

Remote access to the GTCS network is gained only through the Windows VPN (password controlled) – as noted above, there is also access to e-mails via the Office365 portal and via the online portal for restricted information sharing for Panel/Council members. Staff should not attempt to gain access to our networks in any other way.

3.4 Destruction and disposal

All unused 'Data Bearing Devices' (i.e. computer hardware) will be removed and securely destroyed by a certified contractor guaranteeing 100% secure physical destruction. All information held in a physical format (e.g. paper, disc or tape) is subject to similar, secure shredding using our preferred supplier (who attends the office every two weeks to provide this service on-site). 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 member of the CMT).

Authorisation (or permission) is required to destroy certain information, for example a teacher's entry in the Register of Teachers Database, and Senior Managers or Directors should be consulted in relation to this.

4.0 SYSTEM SECURITY

4.1 Networked information systems

4.1.1 Patch Management Policy

All servers are patched on a monthly, ongoing basis by our ICT suppliers.

4.1.2 External infrastructure security testing

External penetration testing is organised on an annual basis and is conducted by external contractors on external facing IP addresses and on the integrity of our information security generally. 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.

4.1.3 Web application testing

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:

- MyGTCS
- Professional Update system
- MyPL system
- Teacher Induction Scheme Profiles
- Flexible Route Profiles
- ITE Profiles
- Student Placement System
- www.gtcs,org.uk website
- www.in2teaching.org.uk website

4.1.4 Payment Card Industry (PCI) Scanning

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.

4.1.5 Virus prevention

Laptop equipment 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. IT support will be responsible for ensuring this process takes place.

Realistic threats to internal systems from viruses come primarily from these sources:

- E-mail attachments

- External storage devices (eg, CDs, USB memory drives, data transferred from mobile phones, or any other media).

- Files/data downloaded from the internet

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 GTCS'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 GCS network unless by agreement with ICT Support who will virus check the device.

Any suspicion that a virus may have entered the system must be reported immediately to our ICT Support suppliers and the Technical Support team. Consideration will then be given to whether there is a potential data incident to be reported in accordance with Annex A.

4.1.6 Back-up processes

GTCS datacentre servers are backed up on a nightly basis. The Clerwood House servers are currently backed up each night using a range of appropriate products. This will soon be changed to a new backup platform when the existing servers have been moved to the new platform at our office in Clerwood House, Edinburgh (as part of the server upgrade project which is currently ongoing).

Replication will also be in place when all existing servers and workloads have been moved to the new platform and will be defined following that.

4.2 Email (Outlook)

4.2.1 General

- Each employee is responsible for all email sent from his or her e-mail account.
- 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.
- All email messages that are created, sent, received or stored on GTCS's email system are the sole property of GTCS.
- All external emails must have GTCS's standard disclaimer set out in them.
- No employee at any level may access the email of another employee without their consent (i.e., they have been granted Delegate access), unless specifically authorised to do so by a member of the Corporate Management Team for business purposes.
- Email inboxes should be cleared out regularly in line with our Records Management and Retention Policy. Save more important emails in the relevant section of the Hub.
- When sharing information internally via email, a link to the information on the Hub should be used rather than sending an attachment as this reduces the duplication of information across the organisation.

4.2.2 Encryption and protection

- GTCS uses appropriate encryption methods via Office 365 Advanced Threat Protection which uses techniques like TLS and Anti-Spoofing to improve email security. Office 365 Advanced Threat Protection protects mailboxes against new, sophisticated malware attacks via unsafe attachments and malicious links.
- Users should consult the Technical Support Team and use the signposted email encryption software or other secure transfer mechanisms, such as CJSM, advised when wishing to transfer information externally via e-mail (or in an electronic format).
- As we cannot guarantee the security of emails once they leave our system, it is not appropriate to send personal or controlled information externally by email unless the information concerned is low risk or appropriate additional security safeguards are put in place. Password protecting documents may be a suitable method for adding a level of security to controlled information. Where information is to be transferred electronically

routinely, a secure information sharing portal should be put in place for use. The signposted email encryption software should be used where it is not worthwhile setting up a secure information sharing portal.

4.2.3 Unacceptable/inappropriate use of email

Unacceptable or inappropriate use of the email system would include but is not limited to:

- Sending harassing, intimidating, abusive, defamatory or offensive materials to or about others.

- Using e-mail for any purpose which violates the law.

- Using email for any of the following:
  - commercial purposes.
  - partisan political purposes.
  - fundraising or charitable activity not sponsored by GTCS.

- Sending viruses.

- Using someone else's identity and password to send messages or misrepresenting your own identity.

- Sending 'chain' or 'pyramid' emails (mail that pointedly urges recipients to spread its contents to others).

- Causing congestion on the network by sending inappropriate messages to specific distribution lists or to all employees.

- Sending unsolicited emails to other companies or individuals. (GTCS E-mail accounts are not allowed to be used for the purpose of sending SPAM messages. Not only is this a misuse of resources, but it can also result in external sites "blacklisting" the GTCS, prohibiting the delivery of any future e-mails to our location. Spamming - is broadly defined as unsolicited E-mail sent to a large number of recipients, and its content is not related to the business.)

- Accessing the Criminal Justice Secure email Service from a device that does not belong to GTCS.

- Accessing unsecure Wi-Fi hotspots for GTCS business. Only secure (require an encrypted pass key) should be used for GTCS business.

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

4.2.4 Personal use of GTCS email

- GTCS email facility should not be used for personal purposes.

- Employees are not permitted to access personal email accounts (e.g., Hotmail, Gmail, Yahoo mail) and social media sites (such as Facebook) from the GTCS network unless required for work purposes. Twitter can be used via an authorised GTCS account.

- Users should not use a non-GTC email account for any GTCS business except to pass business relevant data to their corporate account.

4.2.5 Monitoring

GTCS's electronic communications are monitored to prevent employees from abusing the email and internet systems and to protect GTCS from any legal liability which may arise from this abuse. All monitoring is undertaken in accordance with the Information Commissioner's Code of Practice on Monitoring at Work.

The following general monitoring of overall use is carried out on a regular basis:

- Content checking (i.e., inappropriate words or phrases)
- Address filtering (i.e., where e-mails are sent, forwarded or replied to)

4.3 Internet use

4.3.1 General

We provide internet access for work-related research. The internet is a major source of useful information and, used responsibly, can be a valuable business tool. All employees are therefore encouraged to make full use of it. However, if not careful, browsing the internet, even for business use, can become unfocused and time-consuming. Time spent accessing the web should therefore be kept to sensible and responsible levels.

Employees should also be aware that it is possible to access and download information which may be illegal, and could result in the prosecution of the individual concerned. Employees are restricted from accessing social media sites and personal e-mail from their laptops.

4.3.2 Personal Use

GTCS permits reasonable personal use of the internet provided that this is done out with working hours. A PC in available in the staff room for this purpose. Anyone found to be abusing this privilege may have it withdrawn at any time and the Disciplinary Policy could be invoked.

4.3.3 Inappropriate Material

GTCS utilises software that makes it possible to identify and block access to websites deemed inappropriate by GTCS in the workplace.

The accessing, downloading, possession or sending of pornographic, racist, indecent, offensive or any other distasteful material will be treated as a disciplinary matter. You must notify ICT Support or a member of CMT if you come across information or messages that are inappropriate and make you feel uncomfortable.

4.3.4 Copyright Laws

Much of what appears on the web is protected by copyright. Be aware of the risk of infringing other companies' copyright and other intellectual property rights when downloading or forwarding text, video clips and artistic works or any other software. You must not download or transfer unauthorised copyright photographic, audio or visual files (e.g., desktop wallpapers or MP3 files).

4.3.5 Monitoring

GTCS's electronic communications are monitored to prevent employees from excessive of inappropriate us of internet systems and to protect GTCS from any legal liability which may arise from this. All monitoring is undertaken in accordance with the Information Commissioner's Code of Practice on Monitoring at Work.

The following general monitoring of overall use is carried out on a regular basis:

- Word or phrase filtering i.e. typing inappropriate words into a search engine or on-line forms
- Address filtering i.e. access to inappropriate websites (adult, terrorism, etc)
- Administrator notification of attempted access of blocked sites

Where a line manager believes that an employee may be abusing the email or internet facilities the matter will normally be raised informally with the employee and more specific monitoring may be undertaken and the Disciplinary Policy may be invoked.

Users may be asked to justify their access to a particular site at any time.

4.4 Register of Teachers Database

4.4.1 User access management

User access to all pages on the database is controlled by designated members of the Technical Support Team. Access to the Miller Database 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. Should you no longer require access to a page on the database, you should inform the Senior Manager Digital Development.

User movements are recorded and can be audited and reported on.

4.4.2 Passwords

All users are issued with a Username and Password. It is important that you keep your personal log-on password confidential and safe. Do not disclose them to anyone. Do not use anyone else's password. You will be asked to change your password from time to time for security reasons. Ensure that your passwords are:

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

4.5 CMS (MyGTCS user management)

4.5.1 User access management

A content management system (CMS) is used to manage user accounts for MyGTCS. User access to the CMS is controlled by designated members of the Technical Support Team. Access to CMS is set only for those members of staff who require access to manage accounts for work purposes. Levels of access are set according to individual job remits.

MyGTCS user activity is recorded and can be audited and reported on.

4.5.2 Passwords

All users are issued with a Username and Password. It is important that users keep their personal log-in details confidential and safe. Do not disclose them to anyone. Do not use anyone else's password. Ensure that you change your password from time to time for security reasons. Ensure that your passwords are:

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

5.0 DATA-SPECIFIC SECURITY

5.1 Credit card information

5.2.1 Payments via the Miller database

- Access to credit card data and the credit card payment facility for a user must be authorised by a Senior Manager (or above) and only where this is a business need.
- Users with access to the credit card payment facility will be included in a User Group which will restrict website access as deemed necessary for credit card security in line with PCI DSS compliancy requirements.
- Card holder data is not stored in the database after payment submission. It should not, under any circumstances, be stored anywhere else.
- Access to the card data is available to authorised staff only and is held in a secure location pending processing and then immediate shredding.
- In order to maintain access to the credit card payment facility, users will be required to acknowledge to their line manager annually that they have read, understood and signed this Policy.
- All employees who handle membership credit card information at GTCS will undergo background checks (such as criminal and credit record checks) before they commence this work.

- Changes to security will be applied where necessary to maintain PCI DSS Compliance.

- All third parties with access to credit card account numbers are contractually obligated to comply with card association security standards (PCI/DSS).

5.2.2 Cardholder data

- A list of devices that accept payment card data is maintained.

- Card holder data must never be sent over the internet via email, instant chat or any other end user technologies.

- If there is a business justification to send cardholder data via email or by any other mode then it should be done after authorisation and by using a strong encryption mechanism.

- The transportation of media containing sensitive cardholder data to another location must be authorised by management, logged and inventoried before leaving the premises. Only secure courier service may be used and the status should be monitored until it has been delivered to its new location.

- Attachments should not be sent externally. If you need to share data with external stakeholders this can be done securely. Please discuss this with your line manager.

- In some instances secure remote access can be authorised if you have the need to work away from the office. This can eliminate the need for data transfer entirely.

- If a document is highly confidential or sensitive in nature, you should store it in our document management system, The Hub. When deleting such documents, ensure that you empty your wastebasket as well. Bear in mind that most documents can be accessed by all employees.

- Copies of confidential information should only be printed out as necessary (and retrieved from the printer immediately) and stored or destroyed in an appropriate manner. Shredding is recommended. Locked print recommended.

- portable devices taken out of GTCS premises must not be left unattended and should be locked away, out of sight, when not in use.

- Where a data breach is suspected regarding the transfer or storing of data; including data being lost or damaged or data being seen by, used by, or sent to an unauthorised person, your line manager should be notified straight away and the Data Breach Response Procedure followed.

5.23 Disposal of cardholder data

- All cardholder data must be securely disposed when no longer required by GTCS (as with all other controlled or personal information).

- All hard copies of cardholder data must be manually destroyed by shredding immediately after the card payment has been processed.

- Retention policies should be adhered to for all other data stored on electronic media

5.2.4 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: Business Development
Digital Support Team Leader
Senior Manager: Operations (Student Support)

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 is 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.

5.2 MyGTCS password information

Passwords for MyGTCS should not be transmitted by email. The www.gtcs.org.uk website provides users with the facility to reset their MyGTCS password. This conforms to current best practice.

If a user is unable to use the password reset functionality, a password may be reset by a member of the Technical Support team after the relevant security checks have taken place over the phone.

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

GTCS’s DPO has overall responsibility within GTCS for ensuring that personal data security risks are assessed and mitigated to an acceptable level. The DPO is supported in this role by the GTCS Information Compliance Officer.

The DPO is responsible for ensuring that GTCS complies with all relevant Data Protection Law by providing for the development, maintenance and auditing of GTCS’s information security arrangements. The DPO will ensure that the Senior Management Team and the Council of GTCS 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 GTCS Data Incident Form – Colleague 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 GTCS Data Protection Incident Register.

Data Protection concerns relating to national systems for example the European IMI database that we use or data with joint ownership must be reported directly to the Information Compliance Officer for liaison with other relevant DPOs and where appropriate the UK Information Commissioner.

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 CMT).

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 Corporate Management 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 CMT where practicable, will determine whether a notification is required and if so, to whom.

Under Article 33 of the 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 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 CMT 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 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 publically 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, GTCS 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.

GTCS 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, GTCS 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 GTCS 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, GTCS 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 GTCS 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 GTCS 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 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 GTCS 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, GTCS 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 GTCS 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, GTCS 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, GTCS 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

GTCS through the Corporate Management 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.

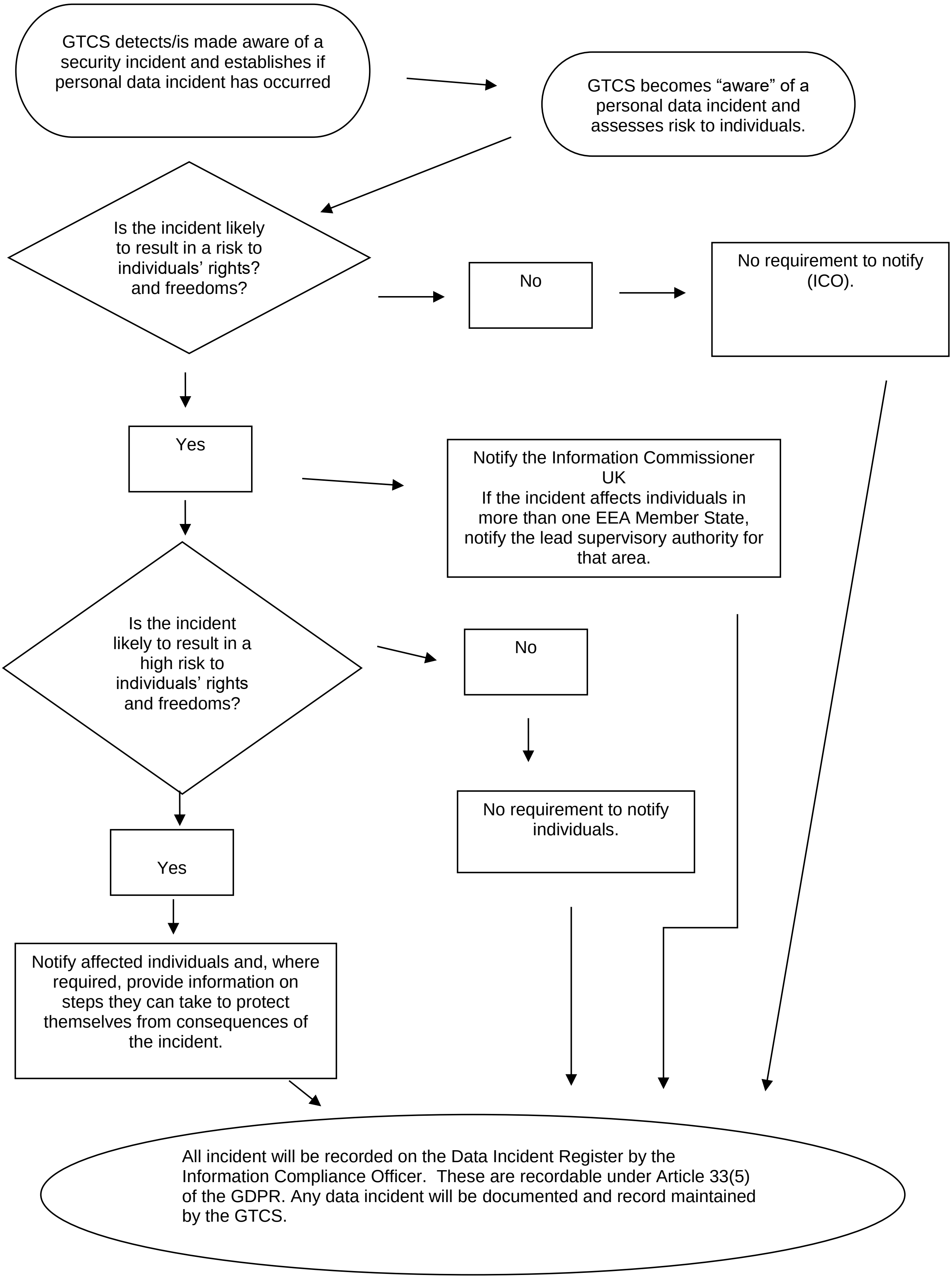
They will also consider whether the GTCS Communications Officer should be informed, to consider how to handle media enquiries or to consider the terms of a press release.

A summary of security breaches will be reported to the Corporate Management Team on each occurrence and where necessary external and regulatory bodies

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

GTCS Data Incident Response Procedure

Flowchart of notification requirements



GTCS detects/is made aware of a security incident and establishes if personal data incident has occurred

GTCS becomes “aware” of a personal data incident and assesses risk to individuals.

Is the incident likely to result in a risk to individuals’ rights? and freedoms?

No

No requirement to notify (ICO).

Yes

Notify the Information Commissioner UK
If the incident affects individuals in more than one EEA Member State, notify the lead supervisory authority for that area.

Is the incident likely to result in a high risk to individuals’ rights and freedoms?

No

No requirement to notify individuals.

Yes

Notify affected individuals and, where required, provide information on steps they can take to protect themselves from consequences of the incident.

All incident will be recorded on the Data Incident Register by the Information Compliance Officer. These are recordable under Article 33(5) of the GDPR. Any data incident will be documented and record maintained by the GTCS.

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.