Information Security & Acceptable Use Policy

Date Approved by Board	February 2024
Next Review Due	November 2024

Contents

1. Introduction and aims 2
2. Relevant legislation and guidance 3
3. Definitions 3
4. Unacceptable use 4
5. Staff (including governors, volunteers, and contractors) 5
6. Children, young people, and vulnerable adults 8
7. Parents/carers 10
8. Data security (Including Passwords, Patching, Anti-Virus, Data Breach & Data Destruction) 11
9. Protection from cyber attacks 18
10. Internet access (including Access Control) 19
11. Monitoring and review (Including Protective Monitoring) 22
12. Related policies 23
Appendix 1: Facebook cheat sheet for staff 24
Appendix 2: Acceptable use of the internet: agreement for parents and carers 26
Appendix 3: Acceptable use agreement for older children, young people, and vulnerable adults 27
Appendix 4: Acceptable use agreement for younger children 29
Appendix 5: Acceptable use agreement for staff, governors, volunteers and visitors 30
Appendix 6: Glossary of cyber security terminology 31
Appendix 7: APTCOO Data Encryption Flow Chart 34
Appendix 8: Record of Changes 34

.....

Introduction and aims

Information and communications technology (ICT) is an integral part of the way APTCOO works and is a critical resource for everyone involved in the business of APTCOO.

However, the ICT resources and facilities APTCOO uses could also pose risks to data protection, online safety, and safeguarding.

This policy aims to:

- Set guidelines and rules on the use of APTCOO ICT resources for staff, children, young people, and vulnerable adults, parents/carers, and governors.
- Establish clear expectations for the way all members of APTCOO community engage with each other online.
- Support APTCOO's policies on data protection, online safety, and safeguarding
- Prevent disruption that could occur to APTCOO through the misuse, or attempted misuse, of ICT systems.
- Support APTCOO in teaching children, young people, and vulnerable adults safe and effective internet and ICT use

This policy covers all users of APTCOO's ICT facilities, including governors, staff, children, young people, and vulnerable adults, volunteers, contractors and visitors.

Breaches of this policy may be dealt with under our staff and/or learner code of conduct and staff disciplinary procedures.

2. Relevant legislation and guidance

This policy refers to, and complies with, the following legislation and guidance:

- Data Protection Act 2018
- The UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020
- Computer Misuse Act 1990
- Human Rights Act 1998
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Education Act 2011
- Freedom of Information Act 2000
- Education and Inspections Act 2006
- Keeping Children Safe in Education 2023
- Searching, screening and confiscation: advice for Schools 2022
- National Cyber Security Centre (NCSC): Cyber Security for Schools
- Education and Training (Welfare of Children) Act 2021
- UK council for internet safety (et al.) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Meeting digital and technology standards in Schools and colleges

3. Definitions

- **ICT facilities:** all facilities, systems and services including, but not limited to, network infrastructure, desktop computers, laptops, tablets, phones, music players or hardware, software, websites, web applications or services, and any device system or service that may become available in the future which is provided as part of APTCOO's ICT service.
- **Users:** anyone authorised by APTCOO to use APTCOO's ICT facilities, including governors, staff, children, young people, and vulnerable adults, volunteers, contractors, and visitors
- **Personal use:** any use or activity not directly related to the users' employment, study or purpose agreed by an authorised user.
- **Authorised personnel:** employees authorised by APTCOO to perform systems administration and/or monitoring of the ICT facilities.

- **Materials:** files and data created using APTCOO's ICT facilities including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites and blogs

See appendix 6 for a glossary of cyber security terminology.

4. Unacceptable use

The following is considered unacceptable use of APTCOO's ICT facilities. Any breach of this policy may result in disciplinary or behaviour proceedings (see section 4.2 below).

Unacceptable use of APTCOO's ICT facilities includes:

- Using APTCOO's ICT facilities to breach intellectual property rights or copyright.
- Using APTCOO's ICT facilities to bully or harass someone else, or to promote unlawful discrimination.
- Breaching APTCOO's policies or procedures
- Any illegal conduct, or statements which are deemed to be advocating illegal activity.
- Online gambling, inappropriate advertising, phishing and/or financial scams
- Accessing, creating, storing, linking to, or sending material that is pornographic, offensive, obscene, or otherwise inappropriate or harmful.
- Consensual and non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams
- Activity which defames or disparages APTCOO, or risks bringing APTCOO into disrepute.
- Sharing confidential information about APTCOO, its children, young people, and vulnerable adults, or other members of APTCOO community
- Connecting any device to APTCOO's ICT network without approval from authorised personnel
- Setting up any software, applications, or web services on APTCOO's network without approval by authorised personnel, or creating or using any programme, tool or item of software designed to interfere with the functioning of APTCOO's ICT facilities, accounts, or data.
- Gaining, or attempting to gain, access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel.
- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to APTCOO's ICT facilities.
- Causing intentional damage to APTCOO's ICT facilities
- Removing, deleting, or disposing of APTCOO's ICT equipment, systems, programmes, or information without permission from authorised personnel
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not permitted by authorised personnel to have access, or without authorisation.

- Using inappropriate or offensive language
- Promoting a private business, unless that business is directly related to APTCOO.
- Using websites or mechanisms to bypass APTCOO's filtering or monitoring mechanisms.
- Engaging in content or conduct that is radicalised, extremist, racist, antisemitic, or discriminatory in any other way.

This is not an exhaustive list. APTCOO reserves the right to amend this list at any time. The Independent Special School headteacher or any other relevant member of staff will use their professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of APTCOO's ICT facilities.

4.1 Exceptions from unacceptable use

Where the use of APTCOO ICT facilities (on APTCOO premises and/or remotely) is required for a purpose that would otherwise be considered an unacceptable use, exemptions to the policy may be granted at the Independent Special School headteacher or any other relevant member of staff's discretion.

4.2 Sanctions

Children, young people, and vulnerable adults and staff who engage in any unacceptable activity, may face disciplinary action in line with APTCOO's codes of conduct.

5. Staff (including governors, volunteers, and contractors)

5.1 Access to APTCOO ICT facilities and materials

APTCOO's IT & Systems Coordinator and Admin & Finance Lead manage access to APTCOO's ICT facilities and materials for APTCOO staff. That includes, but is not limited to:

- Computers, tablets, mobile phones and other devices
- Access permissions for certain programmes or files

Staff will be provided with unique login/account information and passwords that they must use when accessing APTCOO's ICT facilities.

Staff who have access to files that they are not authorised to view or edit, or who need their access permissions updated or changed, should contact the IT & Systems Coordinator or Admin & Finance Lead. Access will be in line with APTCOO's Authorised User policy.

5.1.1 Use of phones and email

APTCOO provides each member of staff with an email address.

This email account should be used for work purposes only. Staff should enable **multi-factor authentication** on their email account(s) in line with APTCOO requirements, selecting from an approved list of methods. Anyone who refuses to enable this process is putting APTCOO's systems at risk and will be subject to disciplinary action.

All work-related business should be conducted using the email address APTCOO has provided.

Staff must not share their personal email addresses with parents/carers and children, young people, and vulnerable adults, and must not send any work-related materials using their personal email account.

Staff must take care with the content of all email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract.

Email messages are required to be disclosed in legal proceedings or in response to requests from individuals under the Data Protection Act 2018 in the same way as paper documents. Deletion from a user's inbox does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable.

Staff must take extra care when sending sensitive or confidential information by email. Any attachments containing sensitive or confidential information should be encrypted so that the information is only accessible by the intended recipient.

If staff receive an email in error, the sender should be informed, and the email deleted. If the email contains sensitive or confidential information, the user must not make use of that information or disclose that information.

If staff send an email in error that contains the personal information of another person, they must inform APTCOO's Data Protection Officer (DPO) immediately and follow our data breach procedure.

Staff must not give their personal phone number(s) to parents/carers or children, young people, and vulnerable adults. Staff must use phones provided by APTCOO to conduct all work-related business.

APTCOO phones must not be used for personal matters.

Staff who are provided with mobile phones as equipment for their role must abide by the same rules for ICT acceptable use as set out in section 4.

5.2 Personal use

Staff are permitted to occasionally use APTCOO ICT facilities for personal use, subject to certain conditions set out below. This permission must not be overused or abused. Senior Leadership may withdraw or restrict this permission at any time and at their discretion.

Personal use is permitted provided that such use:

- Does not take place during contact time/teaching hours.
- Does not constitute 'unacceptable use', as defined in section 4.
- Takes place when no children, young people, and vulnerable adults are present.
- Does not interfere with their jobs, or prevent other staff or children, young people, and vulnerable adults from using the facilities for work or educational purposes.

Staff may not use APTCOO's ICT facilities to store personal, non-work-related information or materials (such as music, videos, or photos).

Staff should be aware that use of APTCOO's ICT facilities for personal use may put personal communications within the scope of APTCOO's ICT monitoring activities (see section 5.5). Where breaches of this policy are found, disciplinary action may be taken.

Staff should be aware that personal use of ICT (even when not using APTCOO ICT facilities) can impact on their employment by, for instance, putting personal details in the public domain, where children, young people, and vulnerable adults and parents/carers could see them.

Staff should take care to follow APTCOO's guidelines on use of social media (see appendix 1, APTCOO's Social Media policy and use of email (see section 5.1.1) to protect themselves online and avoid compromising their professional integrity.

5.2.1 Personal social media accounts

Members of staff should make sure their use of social media, either for work or personal purposes, is always appropriate.

APTCOO has guidelines for staff on appropriate security settings for Facebook accounts (see appendix 1).

5.3 Remote access

We allow staff to access APTCOO's ICT facilities and materials remotely via Intune.

Staff accessing APTCOO's ICT facilities and materials remotely must abide by the same rules as those accessing the facilities and materials on site. Staff must be particularly vigilant if they use APTCOO's ICT facilities outside APTCOO and must take such precautions as the IT & Systems Coordinator may require against importing viruses or compromising system security.

Our ICT facilities contain information which is confidential and/or subject to data protection legislation. Such information must be treated with extreme care and in accordance with our data protection policy.

APTCOO's Data Protection policy can be found on the website.

5.4 APTCOO social media accounts

APTCOO has official 'Facebook' and 'X. Com' accounts, managed by the Admin & Finance Lead and Independent School Headteacher. Staff members who have not been authorised to manage, or post to, the account must not access, or attempt to access, the account.

APTCOO has guidelines for what may and must not be posted on its social media accounts. Those who are authorised to manage, or post to, the account must make sure they always abide by these guidelines.

5.5 Monitoring and filtering of APTCOO network and use of ICT facilities

To safeguard and promote the welfare of children and provide them with a safe environment to learn, APTCOO reserves the right to filter and monitor the use of its ICT facilities and network. This includes, but is not limited to, the filtering and monitoring of:

- Internet sites visited.
- Bandwidth usage
- Email accounts
- Telephone calls
- User activity/access logs

- Any other electronic communications

Only authorised ICT personnel may filter, inspect, monitor, intercept, assess, record and disclose the above, to the extent permitted by law.

APTCOO monitors ICT use in order to:

- Obtain information related to APTCOO business.
- Investigate compliance with APTCOO policies, procedures, and standards.
- Ensure effective APTCOO and ICT operation.
- Conduct training or quality control exercises
- Prevent or detect crime.
- Comply with a subject access request, Freedom of Information Act request, or any other legal obligation.

Our governing board is responsible for making sure that:

- APTCOO meets the DfE's filtering and monitoring standards
- Appropriate filtering and monitoring systems are in place in line with Keeping Children Safe in Education 2023.
- Staff are aware of those systems and trained in their related roles and responsibilities.
    - For the leadership team and relevant staff, this will include how to manage the processes and systems effectively and how to escalate concerns.
- It regularly reviews the effectiveness of APTCOO's monitoring and filtering systems.

APTCOO's designated safeguarding lead (DSL) will take lead responsibility for understanding the filtering and monitoring systems and processes in place.

Where appropriate, staff may raise concerns about monitored activity with APTCOO's DSL and IT & Systems coordinator, as appropriate.

6. Children, young people, and vulnerable adults

6.1 Access to ICT facilities

- Computers and equipment at APTCOO's sites are available to children, young people, and vulnerable adults only under the supervision of staff.
- Young people, and vulnerable adults over the age of 16 can use the computers at Sandy Lane and Tall Trees, independently, for educational purposes only, where agreed by a member of staff and effectively monitored.

6.2 Search and deletion

APTCOO staff can search an individual for any item, with their consent. The ability to give consent may be influenced by the individual's age or other factors; the Headteacher and staff authorised by them have a statutory power to search individual's or their possessions, without consent, where they have reasonable grounds for suspecting that they may have a prohibited item.

Prohibited items include:

- pornographic images
- any article that the member of staff reasonably suspects has been, or is likely to be, used to commit an offence, or to cause personal injury to, or damage to the property of, any person (including the learner).

Confiscation

APTCOO staff can seize any prohibited item found as a result of a search. They can also seize any item, however found, which they consider harmful or detrimental to all within the APTCOO environment. While staff are protected from liability in confiscating and disposing of items, they should always act lawfully, take the situation into context, and consider whether confiscation is appropriate.

Any search carried out will be recorded and evidence taken.

Behaviour and Risk Management Principles and Guidance

APTCOO holds a comprehensive learner context / risk assessment to guide staff around how best to work with a young person to promote positive behaviour, including what to do in the case where management is required for safety. This document will be initiated prior to referral with related historic and current risk indicators, grading of severity and likelihood of behaviour and then detailing how to avoid, divert or manage such behaviour.

Action Taken

- Staff will inform the individual that they are confiscating the device where it is found to have inappropriate images, and will report the incident to the DSL (or deputy) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on searching, screening and confiscation and the UK Council for Internet Safety (UKCIS) et al.'s guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any searching of children, young people, and vulnerable adults will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS et al.'s guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any complaints about searching for, or deleting, inappropriate images or files on children, young people, and vulnerable adults' devices will be dealt with through APTCOO complaints procedure.

6.3 Unacceptable use of ICT and the internet outside of APTCOO

APTCOO will sanction children, young people, and vulnerable adults, in line with the Behaviour for Learning policy if an individual engages in any of the following **at any time** (even if they are not on APTCOO premises):

- Using ICT or the internet to breach intellectual property rights or copyright.
- Using ICT or the internet to bully or harass someone else, or to promote unlawful discrimination.

- Breaching APTCOO's policies or procedures
- Any illegal conduct or making statements which are deemed to be advocating illegal activity.
- Accessing, creating, storing, linking to, or sending material that is pornographic, offensive, obscene or otherwise inappropriate.
- Consensual or non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams (also known as sexting or youth produced sexual imagery)
- Activity which defames or disparages APTCOO, or risks bringing APTCOO into disrepute.
- Sharing confidential information about APTCOO, other children, young people, and vulnerable adults, or other members of APTCOO community
- Gaining or attempting to gain access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel.
- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to APTCOO's ICT facilities.
- Causing intentional damage to APTCOO's ICT facilities or materials
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user and/or those they share it with are not supposed to have access, or without authorisation.
- Using inappropriate or offensive language

7. Parents/carers

7.1 Access to ICT facilities and materials

Parents/carers do not have access to APTCOO's ICT facilities as a matter of course.

However, parents/carers working for, or with, APTCOO in an official capacity (for instance, as a volunteer or as a member of the PTA) may be granted an appropriate level of access or be permitted to use APTCOO's facilities at the headteacher's discretion.

Where parents/carers are granted access in this way, they must abide by this policy as it applies to staff.

7.2 Communicating with or about APTCOO online.

We believe it is important to model for children, young people, and vulnerable adults, and help them learn, how to communicate respectfully with, and about, others online.

Parents/carers play a vital role in helping model this behaviour for their children, especially when communicating with APTCOO through our website and social media channels.

We ask parents/carers to sign the agreement in appendix 2.

7.3 Communicating with parents/carers about individual's activity.

APTCOO will ensure that parents and carers are made aware of any online activity that their children, young people or vulnerable adults are being asked to carry out.

When we ask children, young people, and vulnerable adults to use websites or engage in online activity, we will communicate the details of this to parents/carers in the same way that information about homework tasks is shared.

In particular, staff will let parents/carers know which (if any) person or people from APTCOO children, young people, and vulnerable adults will be interacting with online, including the purpose of the interaction.

Parents/carers may seek any support and advice from APTCOO to ensure a safe online environment is established for their child.

8. Data security (Including Passwords, Patching, Anti-Virus, Data Breach & Data Destruction)

APTCOO is responsible for making sure it has the appropriate level of security protection and procedures in place to safeguard its systems, staff and children, young people, and vulnerable adults. It therefore takes steps to protect the security of its computing resources, data, and user accounts. The effectiveness of these procedures is reviewed periodically to keep up with evolving cyber-crime technologies.

Staff, children, young people, and vulnerable adults, parents/carers and others who use APTCOO's ICT facilities should always use safe computing practices. We aim to meet the cyber security standards recommended by the Department for Education's guidance on digital and technology standards in Schools and colleges, including the use of:

- Firewalls
- Security features
- User authentication and multi-factor authentication
- Anti-malware software

8.1 Passwords

To protect APTCOO systems and data, users must select a password that is secure and difficult to guess. In accordance with security best practice the following rules are enforced:

- All passwords are required to have a minimum of eight characters. Each password must contain a combination of at least three out of the following character sets:
    - Uppercase characters (A through to Z)
    - Lowercase characters (A through to Z)
    - Numerical digits (0 through to 9)
    - Non-alphabetical characters (eg. ! $ # % @ +)
- Previous passwords used for APTCOO systems must not be re-used.
- Passwords must not be something that can easily be guessed through association with yourself (such as using your name, children or a pet's name, car registration number, football team, etc.).
- Password maximum length is not limited by policy and is determined by user preference.

In addition, it is mandatory for users to provide a second factor of authentication for security purposes, with the exception of phone or SMS authentication. Different levels of authentication will be required for different personnel, up to and including multi-factor authentication requirement for each login at an admin account level. Failure to comply in a reasonable manner could lead to system access being restricted to said users.

The password policy will be reviewed annually to ensure that the security posture remains relevant and applicable to technologies, applications and services used by APTCOO.

Users are responsible for the security of their passwords and accounts, and for setting permissions for accounts and files they control.

Members of staff or children, young people, and vulnerable adults who disclose account or password information may face disciplinary action. Parents, visitors, or volunteers who disclose account or password information may have their access rights revoked.

8.2 Software updates, firewalls, patching & anti-virus software

As an element of our business is as an education provider, it is possible that APTCOO could become a target of hackers. In the last few years, attacks on educational establishments have risen considerably.

Hackers try to identify and exploit the vulnerability that each new security update addresses. They try to do this before users are able to update their systems. Unsupported software and hardware are the easiest and most successful vector of attack for hackers. In the last year, several attacks on educational establishments have taken advantage of this, and APTCOO is not immune.

APTCOO is therefore committed to a strong security posture and a key element of this is patching software and hardware as new updates are created.

This policy covers the patching requirements for all systems and applications used within APTCOO. It covers all APTCOO work devices and systems.

APTCOO utilises only properly licensed products with the majority of our work centred within Microsoft licensing through the 365-cloud system. All software end-of-life cycles are followed, and software is uninstalled at the end of its supported period. APTCOO does not and will not use unlicensed hardware or software.

APTCOO uses industry-respected anti-virus and malware products on every device, which is automatically updated as and when new patches become available. The IT & Systems Coordinator keeps track of these updates and ensures that work devices maintain a full protection posture. To ensure this practice is consistent, APTCOO maintains an up-to-date asset register, and educates relevant staff in the importance of regular patching.

APTCOO complete manual updates to hardware or software, including configuration changes, within 14 days of the release of the patch where the vulnerability is:

- described as high risk or worse
- has a Common Vulnerability Scoring System (CVSSv3) score of 7 or above.

The Common Vulnerability Scoring System is the accepted security industry standard for measuring the danger of a vulnerability. The score is a number from 1 to 10 where 10 is the most dangerous.

APTCOO will respond to any alert by the DfE referencing zero-day attacks by patching within 3 days of said warning, should institutions be in danger and a suitable patch available.

If a patch cannot be applied, a different approach to mitigating the risk must instead be developed and approved in writing by the IT & Systems Coordinator in partnership with the SLT.

When a system is not patched in line with this policy, APTCOO reserves the right to take action to secure systems and devices. This includes patching, rebooting, isolating, or disconnecting devices from the network.

When replacing devices and other hardware, APTCOO commits to purchasing systems which are supported and able to receive ongoing updates and maintenance, keeping up to date with the projected life cycles of products as published by the manufacturers and developers of said products.

8.3 Data protection (including data breach and data destruction).

All personal data must be processed and stored in line with data protection regulations and APTCOO's data protection policy.

APTCOO's data protection policy can be found on the website.

Procedures are based on guidance on personal data breaches produced by the Information Commissioner's Office (ICO). It applies to all users of APTCOO systems without exception.

On finding or causing a breach, or potential breach, the staff member, governor, or data processor must immediately notify the data protection officer (DPO) by emailing them at Karen.kilner@aptcoo.org

The DPO will investigate the report and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:

- Lost
- Stolen
- Destroyed
- Altered
- Disclosed or made available where it should not have been.
- Made available to unauthorised people.
- Made unavailable, with a significant negative effect on individuals

Staff and governors will cooperate with the investigation (including allowing access to information and responding to questions). The investigation will not be treated as a disciplinary investigation.

If a breach has occurred or it is considered to be likely that is the case, the DPO will alert the headteacher, the CEO, and the Chair of Governors.

The DPO will make all reasonable efforts to contain and minimise the impact of the breach. Relevant staff members or data processors should help the DPO with this where necessary, and the DPO should take external advice when required (e.g., from IT providers).

The DPO will assess the potential consequences (based on how serious they are and how likely they are to happen) before and after the implementation of steps to mitigate the consequences.

The DPO will work out whether the breach must be reported to the ICO and the individuals affected using the ICO's self-assessment tool

The DPO will document the decision regardless of the decision, in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored in a management-only access folder on APTCOO's Microsoft 365 system.

Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website, or through its breach report line (0303 123 1113), within 72 hours of APTCOO's awareness of the breach. As required, the DPO will set out:

- A description of the nature of the personal data breach including, where possible:
    - The categories and approximate number of individuals concerned.
    - The categories and approximate number of personal data records concerned.
- The name and contact details of the DPO.
- A description of the likely consequences of the personal data breach.

A description of the measures that have been, or will be, taken to deal with the breach and those taken to mitigate any possible adverse effects on the individual(s) concerned.

If all the above details are not yet known, the DPO will report as much as they can within 72 hours of APTCOO's awareness of the breach. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible.

Where APTCOO is required to communicate with individuals whose personal data has been breached, the DPO will tell them in writing. This notification will set out:

- A description, in clear and plain language, of the nature of the personal data breach
- The name and contact details of the DPO
- A description of the likely consequences of the personal data breach
- A description of the measures that have been, or will be, taken to deal with the data breach and those taken to mitigate any possible adverse effects on the individual(s) concerned.
- Any clear and specific advice on how individuals can protect themselves, and what APTCOO is willing to do to help them.

The DPO will consider, in light of the investigation and any engagement with affected individuals, whether to notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies.

The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:

- Facts, including the cause.
- Effects
- Action taken to contain it and make sure it does not happen again (such as establishing more robust processes or providing further training for individuals)

Records of all breaches will be stored in a designated and secure management section of APTCOO's Microsoft 365 system.

The DPO, CEO and headteacher will meet to review what happened and how it can be prevented from happening again. This meeting will happen as soon as reasonably possible.

The DPO, CEO and headteacher will meet at regular intervals to assess recorded data breaches and identify any trends or patterns requiring action by APTCOO to reduce risks of future breaches.

➢ Actions to minimise the impact of data breaches.

We set out below the steps we might take to try to mitigate the impact of different types of data breach if they were to occur, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

Actions taken will include:

- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error.

- Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error.

- If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the IT and System Coordinator to attempt to recall it from external recipients and remove it from the school's email system (retaining a copy if required as evidence)

In any cases where the recall is unsuccessful or cannot be confirmed as successful, the DPO will consider whether it's appropriate to contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save, or replicate it in any way.

The DPO will endeavour to obtain a written response from all the individuals who received the data, confirming that they have complied with this request.

The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted.

If safeguarding information is compromised, the DPO will inform the designated safeguarding lead and discuss whether APTCOO should inform any, or all, of its 3 local safeguarding partners.

Other types of breach that might take place include:

- non-anonymised learner exam results or staff pay information being shared with governors.
- An organisational laptop containing non-encrypted sensitive personal data being stolen or hacked.
- Hardcopy reports sent to the wrong individual's or families.

➢ Data Destruction

This applies to all records, both paper-based and electronic, that are created or collected by APTCOO during the course of its work. Appropriate data destruction is a critical component of data protection and record management policies and processes and must be carried out when the relevant period for retention ends.

- **Who can dispose of data?**

When destroying records internally, APTCOO will liaise with its data protection officer and select the person or people most appropriate for carrying out this process.

If choosing an external provider, make sure the records are shredded on site. The provider should produce a certificate of destruction. Staff working for the external provider should be trained in the handling of confidential documents.

Disposing of paper records

APTCOO will use confidential methods to dispose of hard copies of official records or those containing personal data.

Common appropriate methods include:

- **Open confidential waste bins** for low-level administrative records that don't: contain sensitive personal data; have a business/legal retention period; or require full audit trails. Do not place bins in public areas (e.g. office areas) where anyone can access them. You must label the bin as 'confidential waste' and shred the contents on a regular basis.

- **Office shredding machines** for small quantities or for highly sensitive and confidential documents should be shredded immediately. If possible, use cross-cut or micro-shredders rather than strip-cut shredders as they provide shorter-length strips, and make sure you agree a secure process for using the shredder

- **Secure shredding cabinets.** APTCOO will store records safely until they can be removed for shredding or recycling in a secure office location. APTCOO will empty

the cabinets regularly.

- **Confidential waste sacks.** These bags will be secured (e.g. using a zip tie) and placed in a safe area while awaiting collection. We will create and monitor logs to identify how many bags are awaiting collection and the contents of each bag.

- **Shredding contractors** are the most secure method. **If implemented,** APTCOO must have a contract in place between the data controller (APTCOO) and the processor (the contractor) which outlines their obligations, responsibilities, and liabilities.

Disposing of electronic and other media records

APTCOO will securely delete electronic records containing personal data, and ensure all backups and copies are also deleted.

Before deletion, it will be determined that all legal, business and safeguarding requirements have expired, and that no ongoing litigation or investigation. associated with the data.

If, on rare occasions, we are unable to permanently delete information from electronic systems, it should be **'put beyond use'.**

This means, we will:

- Not use the data for any decision making, or in any way that affects the individual
- Not give the data to another organisation
- Have appropriate security and access controls
- Permanently delete the data if it becomes technically possible

The method of deletion should be suitable to the type of information. Common methods for deleting electronic records include:

- **Deletion** – this is the easiest and most appropriate method for non-confidential records. However, it is important to remember that deletion from a server may not be sufficient, as this only destroys access to the record – e-discovery and recovery tools will still be able to recover the information. To achieve full destruction, APTCOO will aim to use advanced overwriting methods.

- **Overwriting** – this method makes e-discovery and recovery more difficult. APTCOO will follow the recommendations of overwriting using randomised digital code at least three times.

- **Degaussing (for magnetic media) –** this exposes magnetic media, such as tapes and floppy disks, to a magnetic field which scrambles the data beyond use or re-instatement.

- **Physical destruction of the storage media** – physically destroying the media on which the information is stored is widely accepted as the most suitable method for

portable media. Methods include:

- **CDs/DVDs/floppy disks** – should be cut into pieces.
- **Audio/video tapes and fax rolls** – should be dismantled and shredded.
- **Hard disks** – should be dismantled and sanded.
- **USBs** – should be submerged in water and dismantled.

In accordance with ICO and National Cyber Security Centre best practice, APTCOO will utilise an IT asset disposal company that is fully certified with the industry body, the Asset Disposal Information Security Alliance (ADISA) for final disposal purposes.

8.4 Access to facilities and materials

All users of APTCOO's ICT facilities will have clearly defined access rights to APTCOO systems, files, and devices.

These access rights are managed by the IT& Systems Coordinator or the Admin & Finance Lead.

Users should not access, or attempt to access, systems, files, or devices to which they have not been granted access. If access is provided in error, or if something a user should not have access to is shared with them, they should alert the IT & Systems Coordinator or the Admin & Finance Lead immediately.

Users should always log out of systems and lock their equipment when they are not in use to avoid any unauthorised access. Equipment and systems should always be logged out of and shut down completely at the end of each working day.

8.5 Encryption

APTCOO makes sure that its devices and systems have an appropriate level of encryption.

APTCOO staff may only use personal devices (including computers and USB drives) to access APTCOO data, work remotely, or take personal data (such as learner information) out of APTCOO if they have been specifically authorised to do so by the relevant member of the Senior Leadership Team.

Use of such personal devices will only be authorised if the devices have appropriate levels of security and encryption, as defined by the IT & Systems Coordinator.

9. Protection from cyber attacks

Please see the glossary (appendix 6) to help you understand cyber security terminology.

APTCOO will:

- Work with governors and the IT & Systems Coordinator to make sure cyber security is given the time and resources it needs to make APTCOO secure.
- Provide annual training for staff (and include this training in any induction for new starters, if they join outside of APTCOO's annual training window) on the basics of cyber security, including how to:
    - Check the sender address in an email.
    - Respond to a request for bank details, personal information, or login details.
    - Verify requests for payments or changes to information.

- Make sure staff are aware of its procedures for reporting and responding to cyber security incidents.
- Investigate whether our IT software needs updating or replacing to be more secure.
- Not engage in ransom requests from ransomware attacks, as this would not guarantee recovery of data.
- Put controls in place that are:
    - **Proportionate**: APTCOO will verify this using a third-party audit (such as 360 degree safe) at least annually, to objectively test that what it has in place is effective.
    - **Multi-layered**: everyone will be clear on what to look out for to keep our systems safe
    - **Up to date:** with a system in place to monitor when APTCOO needs to update its software
    - **Regularly reviewed and tested**: to make sure the systems are as effective and secure as they can be
- Back up of critical data is automatic on an appropriate external system
- Make sure staff:
    - Enable multi-factor authentication where they can, on things like APTCOO email accounts.
    - Store passwords securely using a password manager.
- Make sure THE It & Systems Coordinator conducts regular access reviews to make sure each user in APTCOO has the right level of permissions and admin rights.
- Have a firewall in place that is switched on.
- Check that its supply chain is secure, for example by asking suppliers about how secure their business practices are and checking if they have the Cyber Essentials certification
- Develop, review and test an incident response plan with the IT department including, for example, how APTCOO will communicate with everyone if communications go down, who will be contacted and when, and who will notify Action Fraud of the incident. This plan will be reviewed and tested, at least annually, and after any significant event has occurred, using the NCSC's 'Exercise in a Box'

10. Internet access (including Access Control)

APTCOO's wireless internet connection is secure.

- We use Talk-Talk filtering.

This section of the policy outlines APTCOO's approach to access control of its data and systems. It provides the guiding principles and responsibilities to ensure the APTCOO's access control objectives are met, and applies to:

- all individuals who have access to APTCOO information and systems.
- all technology and systems that are used to process APTCOO information.
- all information processed, accessed, manipulated, or stored, in any format, by APTCOO in pursuit of its activities.
- internal and external processes used to process APTCOO information.

- all other parties who come into contact with APTCOO data.

Access control

Access to confidential, restricted, and internal information at APTCOO is limited to individuals who require it for work duties, whose job or study responsibilities require it, as determined by our contracts and other agreements, and in line with APTCOO's data protection and acceptable use arrangements.

The responsibility to implement access restrictions lies with the administrators of the APTCOO system in accordance with APTCOO's policies, procedures and agreements.

Role-based access control is used as the method to secure access to all resources. Access rights will be accorded following the principles of least privilege and need-to-know. No uncontrolled external access will be permitted to any network device or system.

Under all circumstances, users of accounts are identifiable, and their activity tied to their accounts.

The allocation of privilege rights (for example, local administrator, domain administrator, super-user, root access) will be restricted, controlled, and not provided by default.

No access to any staff IT resources and services will be provided without prior authentication and authorisation of a user's account. Multi-factor authentication (MFA) will be required for all access.

Access to IT resources and services will be given through the provision of a unique user account and complex password.

Passwords used to access APTCOO systems are a critical part of our identity management and must not be shared. They must comply with APTCOO's password standard, in line with section 8.1 above..

Any user knowing or believing that they have disclosed their account details, or who knows or suspects that their email account has been compromised, must contact the Data Protection Officer and the IT & Systems Coordinator as soon as practicably possible.

Access rights will be reviewed regularly to ensure they remain fit for purpose.

Physical security and physical record storage

Physical files are contained at each site, with the information being relevant to the site's needs on a day-to-day basis. Organisation-wide data is held at APTCOO's main site at Budby. These files are locked away and the keys stored securely. At Budby, these are stored in a secure, password-protected room. Other sites have lockable cabinets in secure rooms accessible only with a key.

All sites themselves are protected by gates and by locked doors which can only be accessed through the use of keys and electronic codes, along with alarm systems which can only be disabled by fobs. Staff members on site are the only people permitted to have and use these fobs.

When people are on site, they are trained to challenge people at the gate who they do not recognise, and to ascertain their identity. Staff also wear lanyards to identify themselves as members of the team.

All visitors, including contractors, are to be met by a member of staff at the door, asked about their business, sign the visitor register, and wear a visitors' badge throughout their time on site.

Digital record storage

All digital records are kept on APTCOO's secure Microsoft 365 system. Information is again on a need-to-know basis, with only information relevant to the individual's level of work being accessible to them.

Financial, management and other sensitive data is restricted further in hidden directories with the same access protocols as listed above.

Onboarding and offboarding

When a new staff member joins APTCOO, they will be provided with an account to access the Microsoft Office 365 system. This will be calibrated to ensure the proper access controls based on their job role, and this will be amended accordingly when job roles change, requiring access to additional data.

Users must comply with the relevant password and multi-factor authentication requirements. If these are not met, their access rights will be removed until the situation is resolved.

At the end of a staff member's tenure with APTCOO, their ability to sign in will be blocked by the administrators and all access links will be disabled, along with a change of password to ensure total inability to access. Accounts will be removed once all relevant emails have been stored for archiving and data retention purposes.

APTCOO will identify all software login details (outside of Microsoft 365) accessible to the person and ensure that they are changed once the individual leaves. We will also ensure that no work devices are in the possession of the individual.

Compliance and breach of policy

APTCOO will conduct cyber security compliance and assurance activities, facilitated by the APTCOO IT & Systems Coordinator to ensure these policy requirements are met. Willful disregard of this policy will be treated extremely seriously by APTCOO and may result in disciplinary measures with the relevant parties.

10.1 Children, young people, and vulnerable adults

- Children, young people and vulnerable adults are given secure access to APTCOO's Wi-fi system; there are relevant filters included as part of the system set up and this is monitored by staff and the IT & Systems Coordinator, in line with the online safety policy and the filtering and monitoring requirements set out in Keeping Children Safe in Education 2023

10.2 Parents/carers and visitors

Parents/carers and visitors to APTCOO will not be permitted to use APTCOO's Wi-Fi unless specific authorisation is granted by the IT & Systems Coordinator.

The IT & Systems Coordinator will only grant authorisation if:

- Parents/carers are working with APTCOO in an official capacity (e.g. as a volunteer)
- Visitors need to access APTCOO's Wi-Fi to fulfil the purpose of their visit (for instance, to access materials stored on personal devices as part of a presentation or lesson plan)

Staff must not give the Wi-Fi password to anyone who is not authorised to have it. Doing so could result in disciplinary action.

11. Monitoring and review (Including Protective Monitoring)

This section covers the monitoring and logging policy and processes APTCOO undertakes regarding its digital systems and infrastructure. This is for the purposes of ensuring data protection, cyber security protocols and compliance with APTCOO policies and procedures.

It applies to:

- all individuals who have access to APTCOO information and systems.
- all tech and systems that are used to process APTCOO information.
- all information processed, accessed, manipulated, or stored, in any format, by APTCOO in pursuit of its activities.
- internal and external processes used to process APTCOO information.
- all other parties who come into contact with APTCOO data and systems.

Capability and procedures

APTCOO can monitor all devices connecting to its systems and networks, including the Microsoft 365 cloud system, firewalls and router logs. This information can be collected and retained, and includes the following:

- Authentication and authorisation attempts, including log-ins and access to files and data.
- IP addresses for location.
- Configuration changes on hardware, including firewalls and routers.
- Device info through Microsoft Entra ID and Intune.
- Additional information is available via Microsoft 365's auditing log system and IT asset register.

All logging is centralised, and logs will be stored in a secure area of the system to minimise the risk of tampering and modification. Write permissions to these files are heavily curated and minimised to ensure only designated personnel can read and access.

The average cyber-attack discovery period is estimated to be 101 days. For these purposes, all logs will be retained for a minimum of 6 months after generation. APTCOO reserves the right to extend this length if it is justified by business need and in line with data protection principles.

All work devices must be connected to the Active Directory to access APTCOO network services and resources. As part of this exchange, control will be exercised over the device (via Intune) for the purposes of security and device management. As part of this, APTCOO will collate audit logs from each device to maintain optimal efficiency and ensure data and system protection.

The IT & Systems Coordinator and the Compliance Lead monitor the implementation of this policy, including ensuring it is updated to reflect the needs and circumstances of APTCOO.

This policy will be reviewed annually.

The governing board is responsible for approving this policy.

12. Related policies

This policy should be read alongside APTCOO's policies on:

- Online safety
- Social media
- Safeguarding and child protection
- Behaviour for learning
- Staff code of conduct
- Data protection & GDPR

Do not accept friend requests from pupils on social media

10 rules for APTCOO staff on Facebook

1. Change your display name – use your first and middle name, use a maiden name, or put your surname backwards instead.
2. Change your profile picture to something unidentifiable, or if you don't, make sure that the image is professional.
3. Check your privacy settings regularly.
4. Be careful about tagging other staff members in images or posts
5. Don't share anything publicly that you wouldn't be happy showing your children.
6. Don't use social media sites during APTCOO hours.
7. Don't make comments about your job, your colleagues, APTCOO or your children, young people, and vulnerable adults online – once it's out there, it's out there.
8. Don't associate yourself with APTCOO on your profile (e.g., by setting it as your workplace, or by 'checking in' at a APTCOO event)
9. Don't link your work email address to your social media accounts. Anyone who has this address (or your personal email address/mobile number) can find you using this information.
10. Consider uninstalling the Facebook app from your phone. The app recognises Wi-Fi connections and makes friend suggestions based on who else uses the same Wi-Fi connection (such as parents or children, young people, and vulnerable adults)

Check your privacy settings.

- Change the visibility of your posts and photos to **'Friends only'**, rather than 'Friends of friends'. Otherwise, children, young people, and vulnerable adults and their families may still be able to read your posts, see things you've shared and look at your pictures if they're friends with anybody on your contacts list
- Don't forget to check your **old posts and photos** – go to bit.ly/2MdQXMN to find out how to limit the visibility of previous posts
- The public may still be able to see posts you've **'liked'**, even if your profile settings are private, because this depends on the privacy settings of the original poster.
- **Google your name** to see what information about you is visible to the public.
- Prevent search engines from indexing your profile so that people can't **search for you by name** – go to bit.ly/2zMdVht to find out how to do this

- Remember that **some information is always public**: your display name, profile picture, cover photo, user ID (in the URL for your profile), country, age range and gender.

What to do if …

An individual adds you on social media.

- In the first instance, ignore and delete the request. Block the learner from viewing your profile.
- Check your privacy settings again and consider changing your display name or profile picture.
- If the learner asks you about the friend request in person, tell them that you're not allowed to accept friend requests from children, young people, and vulnerable adults and that if they persist, you'll have to notify senior leadership and/or their parents/carers. If the learner persists, take a screenshot of their request and any accompanying messages.
- Notify the senior leadership team or the headteacher about what's happening.

A parent/carer adds you on social media.

- It is at your discretion whether to respond. Bear in mind that:
    - Responding to 1 parent/carer's friend request or message might set an unwelcome precedent for both you and other staff at APTCOO.
    - Children, young people, and vulnerable adults may then have indirect access through their parent/carer's account to anything you post, share, comment on or are tagged in.
- If you wish to decline the offer or ignore the message, consider drafting a stock response to let the parent/carer know that you're doing so.

You're being harassed on social media, or somebody is spreading something offensive about you.

- **Do not** retaliate or respond in any way.
- Save evidence of any abuse by taking screenshots and recording the time and date it occurred.
- Report the material to Facebook or the relevant social network and ask them to remove it.
- If the perpetrator is a current learner or staff member, our mediation and disciplinary procedures are usually sufficient to deal with online incidents.
- If the perpetrator is a parent/carer or other external adult, a senior member of staff should invite them to a meeting to address any reasonable concerns or complaints and/or request they remove the offending comments or material.
- If the comments are racist, sexist, of a sexual nature or constitute a hate crime, you or a senior leader should consider contacting the police.

Appendix 2: Acceptable use of the internet: agreement for parents and carers

Acceptable use of the internet: agreement for parents and carers	
Name of parent/carer: **Name of child:**	
Online channels are an important way for parents/carers to communicate with, or about, APTCOO. APTCOO uses the following channels: • Our official Facebook pages. • Email/text groups for parents (for APTCOO announcements and information). Parents/carers also set up independent channels to help them stay on top of what's happening in their child's class. For example, class/year Facebook groups, email groups, or chats (through apps such as WhatsApp).	
When communicating with APTCOO via official communication channels, or using private/independent channels to talk about APTCOO, I will: • Be respectful towards members of staff, and APTCOO, at all times. • Be respectful of other parents/carers and children. • Direct any complaints or concerns through APTCOO's official channels, so they can be dealt with in line with APTCOO's complaints procedure. I will not: • Use private groups, APTCOO's Facebook page, or personal social media to complain about or criticise members of staff. This is not constructive and APTCOO can't improve or address issues unless they are raised in an appropriate way. • Use private groups, APTCOO's Facebook page, or personal social media to complain about, or try to resolve, a behaviour issue involving other children, young people, and vulnerable adults. I will contact APTCOO and speak to the appropriate member of staff if I'm aware of a specific behaviour issue or incident. • Upload or share photos or videos on social media of any child other than my own, unless I have the permission of the other children's parents/carers	
Signed:	**Date:**

Appendix 3: Acceptable use agreement for older children, young people, and vulnerable adults

Acceptable use of APTCOO's ICT facilities and internet: agreement for children, young people, and vulnerable adults and parents/carers	
Name of Individual:	
When using APTCOO's ICT facilities and accessing the internet in APTCOO, I will not: • Use them for a non-educational purpose. • Use them without a teacher being present, or without a member of staff permission. • Use them to break APTCOO rules. • Access any inappropriate websites. • Access social networking sites (unless my teacher has expressly allowed this as part of a learning activity) • Use chat rooms. • Open any attachments in emails, or follow any links in emails, without first checking with a member of staff. • Use any inappropriate language when communicating online, including in emails. • Share any semi-nude or nude images, videos or livestreams, even if I have the consent of the person or people in the photo/video. • Share my password with others or log in to APTCOO's network using someone else's details. • Bully other people. • Use any AI tools and generative chatbots (such as ChatGPT or Google Bard). I understand that APTCOO will monitor the websites I visit and my use of APTCOO's ICT facilities and systems. I will immediately let a member of staff know if I find any material which might upset, distress or harm me or others. I will always use APTCOO's ICT systems and internet responsibly. I understand that APTCOO can discipline me if I do certain unacceptable things online, even if I'm not in APTCOO when I do them.	
Signed:	**Date:**

Parent/carer agreement: I agree that my child can use APTCOO's ICT systems and internet when appropriately supervised by a member of APTCOO staff. I agree to the conditions set out above for children, young people, and vulnerable adults using APTCOO's ICT systems and internet, and for using personal electronic devices in APTCOO, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Appendix 4: Acceptable use agreement for younger children

Acceptable use of APTCOO's ICT facilities and internet: agreement for young children and parents/carers

Name of Individual:

When I use APTCOO's ICT facilities (like computers and equipment) and go on the internet in APTCOO, I will not:

- Use them without asking a staff member first, or without an adult in the room.
- Use them to break APTCOO rules.
- Go on any inappropriate websites.
- Go on Facebook or other social networking sites (unless my tutor said I could as part of a lesson).
- Use chat rooms.
- Open any attachments in emails, or click any links in emails, without checking with a teacher first.
- Use mean or rude language when talking to other people online or in emails.
- Send any photos, videos, or livestreams of people (including me) who aren't wearing all their clothes.
- Share my password with others or log in using someone else's name or password.
- Bully other people.
- Use artificial intelligence (AI) chatbots, such as ChatGPT or Google Bard.

I understand that APTCOO will check the websites I visit and how I use APTCOO's computers and equipment. This is so that they can help keep me safe and make sure I'm following the rules.

I will tell a member of staff I know immediately if I find anything on an APTCOO computer or online that upsets me, or that I know is mean or wrong.

I will always be responsible when I use APTCOO's ICT systems and internet.

I understand that APTCOO can discipline me if I do certain unacceptable things online, even if I'm not in APTCOO when I do them.

Signed :	**Date:**

Parent/carer agreement: I agree that my child can use APTCOO's ICT systems and internet when appropriately supervised by a member of APTCOO staff. I agree to the conditions set out above for children, young people, and vulnerable adults using APTCOO's ICT systems and internet, and for using personal electronic devices in APTCOO, and will make sure my child understands these.

Signed (parent/carer):	**Date:**

Appendix 5: Acceptable use agreement for staff, governors, volunteers and visitors

Acceptable use of APTCOO's ICT facilities and the internet: agreement for staff, governors, volunteers and visitors

Name of staff member/governor/volunteer/visitor:

When using APTCOO's ICT facilities and accessing the internet in APTCOO, or outside APTCOO on a work device, I will not:

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal, or pornographic nature (or create, share, link to or send such material)
- Use them in any way which could harm APTCOO's reputation.
- Access social networking sites or chat rooms
- Use any improper language when communicating online, including in emails or other messaging services.
- Install any unauthorised software or connect unauthorised hardware or devices to APTCOO's network.
- Share my password with others or log in to APTCOO's network using someone else's details.
- Share confidential information about APTCOO, its children, young people, and vulnerable adults or staff, or other members of the community.
- Access, modify or share data I'm not authorised to access, modify or share.
- Promote any private business, unless that business is directly related to APTCOO

I understand that APTCOO will monitor the websites I visit and my use of APTCOO's ICT facilities and systems.

I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside APTCOO, and keep all data securely stored in accordance with this policy and APTCOO's data protection policy.

I will let the designated safeguarding lead (DSL) and IT &Systems Coordinator know if an individual informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.

I will always use APTCOO's ICT systems and internet responsibly, and ensure that children, young people, and vulnerable adults in my care do so too.

Signed (staff member/governor/volunteer/visitor):	**Date:**

Appendix 6: Glossary of cyber security terminology

These key terms will help you to understand the common forms of cyber-attack and the measures APTCOO will put in place. They're from the National Cyber Security Centre (NCSC) glossary.

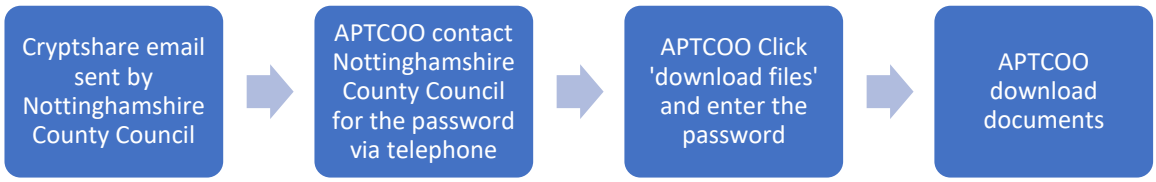
TERM	DEFINITION
Antivirus	Software designed to detect, stop and remove malicious software and viruses.
Breach	When your data, systems or networks are accessed or changed in a non-authorised way.
Cloud	Where you can store and access your resources (including data and software) via the internet, instead of locally on physical devices.
Cyber attack	An attempt to access, damage or disrupt your computer systems, networks or devices maliciously.
Cyber incident	Where the security of your system or service has been breached.
Cyber security	The protection of your devices, services and networks (and the information they contain) from theft or damage.
Download attack	Where malicious software or a virus is downloaded unintentionally onto a device without the user's knowledge or consent.
Firewall	Hardware or software that uses a defined rule set to constrain network traffic – this is to prevent unauthorised access to or from a network.
Hacker	Someone with some computer skills who uses them to break into computers, systems and networks.
Malware	Malicious software. This includes viruses, trojans or any code or content that can adversely impact individuals or organisations.

TERM	DEFINITION
Patching	Updating firmware or software to improve security and/or enhance functionality.
Pentest	Short for penetration test. This is an authorised test of a computer network or system to look for security weaknesses.
Pharming	An attack on your computer network that means users are redirected to a wrong or illegitimate website even if they type in the right website address.
Phishing	Untargeted, mass emails sent to many people asking for sensitive information (such as bank details) or encouraging them to visit a fake website.
Ransomware	Malicious software that stops you from using your data or systems until you make a payment.
Social engineering	Manipulating people into giving information or carrying out specific actions that an attacker can use.
Spear-phishing	A more targeted form of phishing where an email is designed to look like it's from a person the recipient knows and/or trusts.
Trojan	A type of malware/virus designed to look like legitimate software that can be used to hack a victim's computer.
Two-factor/multi-factor authentication	Using 2 or more different components to verify a user's identity.
Virus	Programmes designed to self-replicate and infect legitimate software programs or systems.
Virtual private network (VPN)	An encrypted network which allows remote users to connect securely.

TERM	DEFINITION
Whaling	Highly- targeted phishing attacks (where emails are made to look legitimate) aimed at senior people in an organisation.

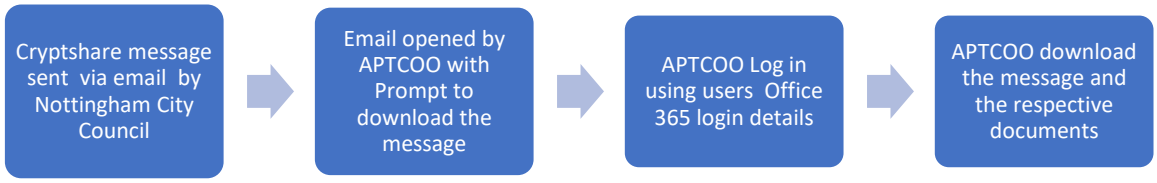
APTCOO Receiving Information/Data:

1. Nottinghamshire County Council specific:

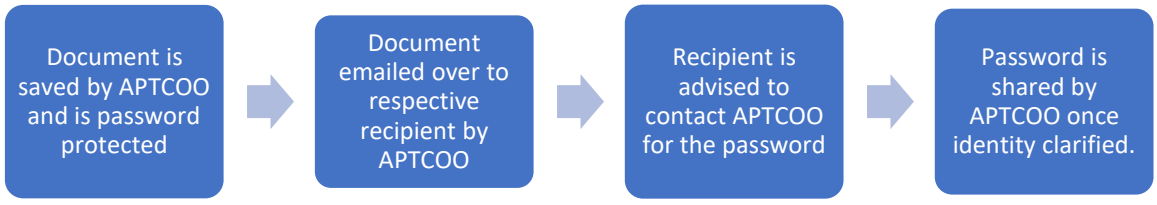


OR

2. Nottingham City Council Specific:



APTCOO Sending Information/Data:



Appendix 8:

RECORD OF CHANGES: Information Security and Acceptable Use Policy

DATE	AUTHOR	PROCEDURE	DETAILS OF CHANGE
08/11/2023	Compliance Lead	Update of policy from the Acceptable Use policy (V1 created Sept 23)	Version 2 created as part of the Information Security review November 2023. (Adapted Key Leaders template policy) and inclusion of Appendix 7 (Data encryption/receiving and sending documentation process map)
22/11/2023	Compliance Lead	Incorporation of various individual IT policies into Information Security and Acceptable Use policy	Incorporation of following policies into the Information Security and Acceptable Use Policy (V2): • Access Control Policy • Data Breach Policy • Data Destruction Policy • Password Policy • Patching & Anti-Virus Policy • Protective Monitoring Policy
