Network and IT Security Policy

1. Contents

1. Contents 2
2. Version control 3
3. Statement of intent 4
4. Legal framework 4
5. Types of security breach and causes 4
6. Roles and responsibilities 5
7. Secure configuration 6
8. Network security 7
9. Virus and malware prevention 7
10. User privileges 7
11. Monitoring usage 8
12. Removable media controls and home working 9
13. Backing-up data 9
14. Avoiding phishing attacks 9
15. User training and awareness 10
16. Data security breach incidents 10
17. IT Disaster Recovery Plan 11
18. Monitoring & Review 11

2. Version control

Date	Version	Revision	Owner
15/06/20	1.0	New Policy (and replaces IT Disaster Recovery Plan)	Future Generation Trust Policy Team

3. Statement of intent

Future Generation Trust is committed to maintaining the confidentiality of its information and ensuring that the details of the finances, operations and individuals within the Trust are only accessible by the appropriate individuals. It is, therefore, important to uphold high standards of security, take suitable precautions, and to have systems and procedures in place that support this.

Future Generation Trust recognises, however, that breaches in security can occur, particularly as most information is stored online or on electronic devices which are increasingly vulnerable to cyber-attacks. This being the case, it is necessary to have a contingency plan containing a procedure to minimise the potential negative impacts of any security breach, to alert the relevant authorities, and to take steps to help prevent a repeat occurrence.

4. Legal framework

This policy has due regard to statutory legislation and advisory guidance including, but not limited to, the following:

- Computer Misuse Act 1990
- General Data Protection Regulation 2018
- National Cyber Security Centre – 'Cyber Security: Small Business Guide' 2018

This policy has due regard to the Trust's policies and procedures including, but not limited to:

- Business Continuity Plans
- CCTV Policy
- Data Breach Notification Policy
- Data Protection Policy
- E-Safety Policy (including Acceptable Use Agreements)
- Records Management Policy
- Risk Management Policy

5. Types of security breach and causes

Unauthorised use without damage to data – involves unauthorised persons accessing data on the Trust systems, e.g. 'hackers', who may read the data or copy it, but who do not actually damage the data in terms of altering or deleting it.

Unauthorised removal of data – involves an authorised person accessing data, who removes the data to pass it on to another person who is not authorised to view it, e.g. a staff member with authorised access who passes the data on to a friend without authorised access – this is also known as data theft. The data may be forwarded or deleted altogether.

Damage to physical systems – involves damage to the hardware in the Trust's ICT system, which may result in data being inaccessible to the Trust or academy and/or becoming accessible to unauthorised persons.

Unauthorised damage to data – involves an unauthorised person causing damage to data, either by altering or deleting it. Data may also be damaged by a virus attack, rather than a specific individual.

Breaches in security may be caused as a result of actions by individuals, which may be accidental, malicious or the result of negligence – these can include:

- Accidental breaches, e.g. as a result of insufficient training for staff, so they are unaware of the procedures to follow.
- Malicious breaches, e.g. as a result of a hacker wishing to cause damage to the Trust or academy through accessing and altering, sharing or removing data.
- Negligence, e.g. as a result of an employee that is aware of Trust policies and procedures, but disregards these.

Breaches in security may also be caused as a result of system issues, which could involve incorrect installation, configuration problems or an operational error – these can include:

- Incorrect installation of anti-virus software and/or use of software which is not the most up-to-date version, meaning the Trust or academy software is more vulnerable to a virus.
- Incorrect firewall settings are applied, e.g. access to the Trust or academy network, meaning individuals other than those required could access the system.
- Confusion between backup copies of data, meaning the most recent data could be overwritten.

6. Roles and responsibilities

The Data Protection Officer (DPO) is responsible for:

- The overall monitoring and management of data security.
- Deciding which strategies are required for managing the risks posed by internet use, and for keeping the Trust's network services, data and users safe, in conjunction with the Learning Technologies Manager.
- Leading on the Trust's response to incidents of data security breaches.
- Assessing the risks to the Trust in the event of a data security breach.
- Producing a comprehensive report following a full investigation of a data security breach.
- Determining which organisations and individuals need to be notified following a data security breach, and ensuring they are notified as outlined in the Trust's **Data Breach Notification Policy**.
- In the event of any data security breach to determine where weaknesses lie and improve security measures.
- Organising training for staff members on data security and preventing breaches.
- Monitoring the effectiveness of this policy, alongside the Learning Technologies Manager and Headteachers, and communicating any changes to staff members.

The managed IT service (provided by Entrust) or the Learning Technologies Manager are responsible for:

- Maintaining an inventory of all ICT hardware and software currently in use within the Trust.
- Ensuring any software that is out-of-date is removed from the academy premises.
- Implementing effective firewalls to enhance network security and ensuring that these are monitored regularly.
- Ensuring all Trust-owned devices have secure virus and malware protection and that devices are regularly updated.
- Installing, monitoring and reviewing filtering systems for the Trust's network(s).

- Setting up user privileges in line with recommendations from the Headteacher and maintaining a written record of privileges.
- Maintaining an up-to-date inventory of all usernames.
- Removing any inactive users from the Trust's systems, ensuring that this is always up-to-date.
- Recording any alerts for access to inappropriate content and notifying the relevant Headteacher(s).
- Performing a back-up of all electronic data held by the Trust, ensuring detailed records of findings are kept.

The Headteacher is responsible for:

- Ensuring all staff members and pupils are aware of their responsibilities in relation to this policy.
- Defining users' access rights for both staff and pupils.
- Responding to alerts for access to inappropriate content in line with the Trust's **E-Safety Policy**.
- Informing the managed IT service or the Learning Technologies Manager of staff members who are permitted to use their personal devices for work purposes so that appropriate security methods can be applied.
- Issuing disciplinary sanctions to pupils or members of staff who cause a data security breach.
- Organising training for staff members on network and IT security in conjunction with the managed IT service or the Learning Technologies Manager and the Data Protection Officer.

7. Secure configuration

An inventory will be kept of all ICT hardware and software currently in use within the Trust, including portable devices.

Any changes to the ICT hardware or software will be documented using the inventory and will be authorised by the managed IT service or Learning Technologies Manager before use.

All systems will be audited on a termly basis by the managed IT service or the Learning Technologies Manager to ensure the software is up-to-date. Any new versions of software or new security patches will be added to systems, ensuring that they do not affect network security, and will be recorded in the inventory.

Any software that is out-of-date or reaches its 'end of life' will be removed from systems, i.e. when suppliers end their support for outdated products such that any security issues will not be rectified.

All hardware, software and operating systems will require passwords from individual users before use. Passwords will be changed at the start of each academic year to prevent access to facilities which could compromise network security.

Future Generation Trust believes that locking down hardware, such as through the use of strong passwords, is an effective way to prevent access to facilities by unauthorised users.

8. Network security

Future Generation Trust will employ firewalls in order to prevent unauthorised access to the systems.

The Trust's firewall is deployed as a centralised system which is controlled by a third party. The broadband service connects to a firewall that is located within a data centre or other major network location.

9. Virus and malware prevention

Future Generation Trust understands that viruses and malware can be damaging for network security and may enter the network through a variety of means, such as email attachments, social media, malicious websites or removable media controls.

The managed IT service or the Learning Technologies Manager will ensure that all Trust devices have secure virus and malware protection and undergo regular scans in line with specific requirements.

The managed IT service or the Learning Technologies Manager will update virus and malware protection on a regular basis to ensure it is up-to-date and can react to changing threats.

Virus and malware protection will also be updated in the event of any attacks to the Trust's hardware and software.

Filtering of websites, as detailed in section 10 of this policy, will ensure that access to websites with known malware are blocked immediately and reported to the managed IT service or the Learning Technologies Manager.

The Trust will use mail security technology, which will detect and block any malware that is transmitted by email. This will also detect any spam or other messages which are designed to exploit users.

The managed IT service or the Learning Technologies Manager will review the mail security technology on a regular basis to ensure it is kept up-to-date and effective.

10. User privileges

Future Generation Trust understands that controlling what users have access to is important for promoting network security. User privileges will be differentiated, i.e. pupils will have different access to data and the network than members of staff.

The managed IT service or the Learning Technologies Manager will ensure that user accounts are set up to allow users access to the facilities required, in line with the Headteacher's instructions, whilst minimising the potential for deliberate or accidental attacks on the network.

The managed IT service or the Learning Technologies Manager will ensure that websites are filtered for inappropriate and malicious content.

All users will be required to change their passwords at the start of each academic year and will use upper and lowercase letters, as well as numbers, to ensure that passwords are strong.

Users will also be required to change their password if they become known to other individuals.

Pupils are responsible for remembering their passwords; however, the managed IT service or the Learning and Technologies Manager will have an up-to-date record of all usernames and will be able to reset them if necessary.

Only the managed IT service or the Learning Technologies Manager has access to the record of usernames.

Pupils from Reception to Year 6 have individual logins and use a generic password.

The 'master user' password used by the managed IT service and/or the Learning Technologies Manager will also be made available to the Headteacher and Data Protection Officer.

The master user account is subject to a two-factor authentication for logins. This account requires two different methods to provide identity before logging in – these are:

- A password; and a
- Code sent to another device, such as a tablet or mobile phone, which must be entered following the password.

The master user account is used as the 'administrator' which allows designated users to make changes that will affect other users' accounts in the Trust, such as changing security settings, monitoring use, and installing software and hardware.

User provisioning systems will be employed in order to delete inactive users or users who have left the Trust. The managed IT service or the Learning Technologies Manager will manage this provision to ensure that all users that should be deleted are, and that they do not have access to the system.

The managed IT service or the Learning Technologies Manager will review the system on a termly basis to ensure the system is working at the required level.

11. Monitoring usage

Monitoring user activity is important for the early detection of attacks and incidents, as well as inappropriate usage by pupils or staff.

Future Generation Trust will inform all pupils and staff that their usage will be monitored, in accordance with the Trust's **E-Safety Policy** (including Acceptable Use Agreements).

If a user accesses inappropriate content or a threat is detected, an alert will be sent to the managed IT service or the Learning Technologies Manager. Alerts will also be sent for unauthorised and accidental usage. Alerts will identify the user, the activity that prompted the alert and the information or service the user was attempting to access.

The managed IT service or the Learning Technologies Manager will record any alerts using an incident log and will report this to the Headteacher(s). All incidents will be responded to in accordance with the Trust's **E-Safety Policy**.

All data gathered by monitoring usage will be kept in accordance with the Trust's **Records Management Policy**. This data may be used as a method of evidence for supporting a not yet discovered breach of network security. In addition, the data may be used to ensure the Trust is protected and all software is up-to-date.

12. Removable media controls and home working

Future Generation Trust understands that staff may need to access the Trust network from areas other than on the premises. Effective security management will be established to prevent access to, or leakage of, data, as well as any possible risk of virus or malware.

Before distributing any Trust-owned devices, the managed IT service or the Learning Technologies Manager will ensure that manufactures' default passwords have been changed. A set password will be chosen and the staff member will be prompted to change the password once using the device.

When using laptops, tablets and other portable devices, the Headteacher will determine the limitations for access to the network.

Staff who use Trust-owned laptops, tablets and other portable devices will use them for work purposes only, whether on or off academy premises.

Staff members will avoid connecting to unknown Wi-Fi hotspots, such as in coffee shops, when using any laptops, tablets or other devices.

All data will be held on systems centrally in order to reduce the need for the creation of multiple copies, and/or the need to transfer data using removable media controls.

The Wi-Fi network at each academy will be password protected and will only be given out as required. Staff and pupils are not permitted to use the Wi-Fi for their personal devices, such as mobile phones or tablets, unless instructed otherwise by the Headteacher.

13. Backing-up data

Where possible, back-ups are run overnight and are completed before the beginning of the next school day.

Upon completion of back-ups, data is stored on the Trust's hardware which is password protected.

Only authorised personnel are able to access the Trust's data.

14. Avoiding phishing attacks

The managed IT service or the Learning Technologies Manager will configure all staff accounts using the principle of 'least privilege' – staff members are only provided with as much rights as are required to perform their jobs.

Two-factor authentication is used on any important accounts, such as the master user account, Chief Executive Officer, Headteachers, Head of Finance and HR and Finance Officer.

In accordance with section 15 of this policy, the managed IT service or the Learning Technologies Manager and Headteacher will organise regular training for staff members – this will cover identifying irregular emails in order to help staff members spot requests that are out of the ordinary, such as receiving an invoice for a service not used, and who to contact if they notice anything unusual.

Staff will use the following warning signs when considering whether an email may be unusual:

- Is the email from overseas?
- Is the spelling, grammar and punctuation poor?
- Is the design and quality what you would expect from a large organisation?
- Is the email addressed to a 'valued customer', 'friend' or 'colleague'?
- Does the email contain a veiled threat that asks the staff member to act urgently?
- Is the email from a senior member of the Trust or academy asking for a payment?
- Does the email sound too good to be true? It is unlikely someone will want to give another individual money or access to another service for free.

The managed IT service or the Learning Technologies Manager will ensure that email filtering systems, applied in accordance with section 9 of this policy, are neither too strict or lenient; filtering that is too strict may lead to legitimate emails becoming lost, and too lenient filters may mean that emails that are spam or junk are not sent to the relevant folder.

To prevent hackers having access to unnecessary public information, the Data Protection Officer will ensure the Trust's social media accounts and websites are reviewed on a regular basis, making sure that only necessary information is shared.

The Trust's **E-Safety Policy** includes expectations for sharing of information – and determines what is and is not necessary to share.

The Headteacher will ensure parents, pupils, staff and other members of the school community are aware of acceptable use of social media and the information they share about the academy and themselves, in accordance with the Trust's **E-Safety Policy**.

15. User training and awareness

The Headteacher will arrange training for pupils and staff to ensure they are aware of how to use the network appropriately in accordance with the Trust's **E-safety Policy** (including Acceptable Use Agreements).

Through training, all pupils and staff will be aware of who they should inform first in the event that they suspect a data security breach, and who they should inform if they suspect someone else is using their passwords.

All staff will receive training on the contents of this policy as part of their induction programme. Any new pupils who join the academy part way through an academic year will be briefed on e-safety.

All users will be made aware of the disciplinary procedures for the misuse of the network leading to malicious attacks, in accordance with the process detailed in the Trust's **E-Safety Policy**.

16. Data security breach incidents

In the event of any suspected or identified data security breach incidents staff should follow the guidance detailed in the Trust's **Data Breach Notification Policy**.

17. IT Disaster Recovery Plan

The ongoing availability of important data is critical to the effective operation of Future Generation Trust. The procedures detailed within this policy are designed to minimise the potential loss or corruption of this data. In addition, they also ensure that secure back-up arrangements are in place which is paramount should the recovery of important data be required.

In the event that either IT, communications or data need to be re-instated or recovered as a result of an incident each academy will follow the documented recovery process outlined in their site specific **Business Continuity Plans**.

18. Monitoring & Review

The Future Generation Trust Board has overall responsibility for this policy and for reviewing its content and effectiveness.

The Data Protection Officer, the managed IT service, the Learning Technologies Manager and Headteachers have operational responsibility for implementation and must ensure that staff and pupils are suitably briefed and trained on its content with regard to their responsibilities.

This policy and all arrangements and procedures will be reviewed annually.

Policy adopted on: **1 July 2020**

Review date: **July 2021**

Signed: Fliss Dale **Designation:** Chair of Trust Board