THE JUBILEE ACADEMY

Aspire and Achieve

Title:	**E-Safety and ICT Acceptable Use Policy in. of Remote and Mobile Technology**
Date Approved:	**July 2013**
Date Reviewed:	**August 2021**
Status:	**Non-Statutory**
Delegation:	**Head of School**
Responsibility:	**SBM H&S and IT Technician**
Review Frequency:	**Annually**
Policy Locations:	**Website/Staff Shared Drive/Hard Copy**
Next Review Date:	**August 2022**

E-Safety and ICT Acceptable Use Policy

Statement of intent

This policy has been developed to ensure that all adults at The Jubilee Academy are working together to safeguard and promote the welfare of young people.

E-Safety is a safeguarding issue not an ICT issue and all members of the school community have a duty to be aware of e-safety at all times, to know the required procedures and to act on them.

This document aims to put into place effective management systems and arrangements which will maximise the educational and social benefit that can be obtained by exploiting the benefits and opportunities of using ICT, whilst minimising any associated risks. It describes actions that should be put in place to redress any concerns about student welfare and safety as well as how to protect young people and staff from risks and infringements.

The Head of School or, in their absence, the authorised member of staff for e-safety has the ultimate responsibility for safeguarding and promoting the welfare of students in their care.

The purpose of internet use in school is to help raise educational standards, promote student achievement, and support the professional work of staff as well as enhance the school's management information and business administration systems.

The internet is an essential element in 21st century life for education, business and social interaction and the school has a duty to provide young people with quality access as part of their learning experience and curriculum.

A risk assessment will be carried out before young people are allowed to use new technology in the school.

Ethos

- It is the duty of the school to ensure that every student in its care is safe. The same 'staying safe' outcomes and principles outlined in Every Child Matters agenda apply equally to the 'virtual' or digital world;
- Safeguarding and promoting the welfare of students is embedded in the culture of the school and its everyday practice and procedures;
- All staff have a responsibility to support e-Safe practices in school and all students need to understand their responsibilities in the event of deliberate attempts to breach e-safety protocols;
- E-safety is a concern that is not limited to school premises, school equipment or the school day;
- Bullying, harassment or abuse of any kind via digital technologies or mobile phones will not be tolerated and complaints of cyber-bullying will deal with in accordance with the school's policies on behaviour and preventing and responding to bullying;
- Complaints related to child protection will be dealt with in accordance with the school's child protection policy.

The Head of School of The Jubilee Academy will ensure that:

- All staff should be included in E-Safety training. Staff must also understand that misuse of the internet may lead to disciplinary action (as detailed in section 5 of the HR Policies) and possible dismissal;
- A Designated Senior Member of Staff for E-learning /Safety is identified and receives

appropriate on-going training, support and supervision and works closely with the Designated Person for Child Protection;
- All temporary staff and volunteers are made aware of the school's E-learning /Safety Policy and arrangements;
- A commitment to E-Safety is an integral part of the safer recruitment and selection process of staff and volunteers.

The Governing Body will ensure that:
- There is a senior member of the school's leadership team who is designated to take the lead on e-learning/safety within the school;
- This Policy is reviewed as required
- Procedures are in place for dealing with breaches of e-safety and security;
- The Business Continuity plan links to this policy and offers strategic direction for cyber threats
- All staff and volunteers have access to appropriate ICT training.

Designated Esafety Lead(s) will ensure that:
- Developing an e-Safe culture throughout the setting as part of safeguarding, which is in line with national best practice recommendations (e.g. Ofsted, DfE)
- Ensuring that e-Safety is clearly identified and established as part of the roles and responsibility of the management/senior leadership team and governing body etc
- Acting as a named point of contact on all e-Safety issues and liaising with other members of staff as appropriate
- Keeping up-to-date with current research, legislation and trends. This may include accessing appropriate training and using a range of approaches to enable them to understand the role of new technology as part of modern British society and the wider safeguarding agenda.
- Leading an e-Safety team with input from all stakeholder groups.
- Embedding e-Safety in staff training and CPD by ensuring that all members of staff receive upto-date and appropriate e-Safety training (at least annually and as part of induction) which sets out clear boundaries for safe and professional online conduct
- Ensuring that there is an age and ability appropriate e-Safety curriculum that is embedded, progressive, flexible and relevant which engages children's' interest and promotes their ability to use technology responsibly and to keep themselves and others safe online
- Ensuring that the setting participates in local and national events to promote positive online behaviour, e.g. Safer Internet Day
- Ensuring that e-Safety is promoted to parents and carers and the wider community through a variety of channels and approaches
- Ensuring there are robust reporting channels for the community to access regarding e-Safety concerns, including internal, local and national support.
- To ensure that age-appropriate filtering is in place, which is actively monitored
- Ensure that appropriate risk assessments are undertaken regarding the safe use of technology, including ensuring the safe and responsible use of devices
- Work with the lead for data protection and data security to ensure that practice is in line with legislation
- Maintaining an e-Safety incident/action log to record incidents and actions taken.
- Liaising with the local authority and other local and national bodies as appropriate.
- Reviewing and updating e-Safety policies, Acceptable Use Policies and other procedures on a regular basis (at least annually) with stakeholder input and ensuring that e-Safety is integrated with other appropriate school policies and procedures.
- Monitoring and reporting on e-Safety issues to the school management team, Governing Body and other agencies as appropriate

Teaching and learning

Benefits of internet use for education:
- The internet is a part of the statutory curriculum and a necessary tool for staff and students and it benefits education by allowing access to the world - wide educational resources including art galleries and museums as well as enabling access to specialists in many fields for students and staff;
- Access to the internet supports educational and cultural exchanges between students worldwide and enables students to participate in cultural, vocational, social and leisure use in libraries, clubs and at

home;

- The internet supports professional development for staff through access to national developments, educational materials, good curriculum practice and exchange of curriculum and administration data;
- The internet improves access to technical support, including remote management of networks, supports communication with support services, professional associations and colleagues as well as allowing access to, and inclusion in, government initiatives;
- The internet offers opportunities for mentoring students and providing peer support for them and their teachers;
- Students will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation;
- Students will be encouraged to question what they read and to seek confirmation of matters of fact from more than one source. They will be taught research techniques including the use of subject catalogues and search engines and encouraged to question the validity, currency and origins of information. Students will also be taught that copying material is worth little without an appropriate commentary demonstrating the selectivity used and evaluating the material's significance;
- Students will be taught to acknowledge the source of information used and to respect copyright when using internet material in their own work.

Managing the internet

- To control malvertising the school has internet filter installed to ensure computers are not compromised when staff hover on or click on what looks like and advert
- Developing good practice in internet use as a tool for teaching and learning is essential. The School internet access will be designed expressly for student use and will include filtering appropriate to the age of the young people;
- Students will be taught what internet use is acceptable and what is not and be given clear objectives for internet use. Staff will guide students in on-line activities in class that will support the learning outcomes planned for the student's age and maturity;
- Students will be taught what to do if they experience material that they find distasteful, uncomfortable or threatening;
- If staff or students discover unsuitable sites, the URL (address) and content must be reported to the ICT Technician and Senior member of staff;
- The School will ensure that the use of Internet derived materials by staff and students complies with copyright law;
- Students will be taught to be critically aware of the materials they read as well as how to validate information before accepting its validity;

Managing email

- The school uses Microsoft Outlook email service which has a spam filter to respond to spam
- All staff must read and sign a copy of the Safe Working Practice Agreement Safeguarding Students and Young People and school's 'Acceptable Use of ICT Resources' document before being allowed controlled access to this email service
- All Students must read and sign a copy of the school's 'Acceptable Use of ICT Resources' document before being allowed controlled access to this email service
- Personal e-mail or messaging between staff and students should not take place;
- Staff must use the School e-mail address if they need to communicate with students about their School work e.g. study leave, course work and only fully trained e-mentors should contact students via email and only ever using the appropriate medium through Microsoft Teams;
- Students and staff may only use approved e-mail accounts on the school system and students must inform a member of staff immediately if they receive an offensive e-mail;
- Students must not reveal details of themselves or others in any e-mail communication or by any personal web space such as an address, telephone number and must not arrange meetings with anyone;
- Access in School to external personal e-mail accounts may be blocked;
- Excessive social email use can interfere with learning and will be restricted;
- The forwarding of chain letters is not permitted;
- Incoming email should be monitored, and attachments should not be opened unless the author is known to minimise threat to viruses and phishing emails
- Training on induction and Esafety training provide staff with continuous guidance

- Email best practice guidance available to all staff

Managing website content

- Editorial guidance will ensure that the school's ethos is reflected in the website, information is accurate, well presented and personal security is not compromised. Care will be taken to ensure that all information is considered from a security viewpoint including the use of photographic material;
- Photographs of students and teachers will not be used without the written consent of the student's parents/carers in line with the GDPR;
- The point of contact on the school website will be the school address, School email and telephone number. Staff or students' home information will not be published;
- The Head of School or nominated person will have overall editorial responsibility and ensure that all content is accurate and appropriate;
- The website will comply with the school's guidelines for publications and parents/carers will be informed of the school policy on image taking and publishing;
- Use of site photographs will be carefully selected so that any students cannot be identified, or their image misused;
- The names of students will not be used on the website, particularly in association with any photographs;
- Work will only be used on the website with the permission of the student and their parents/carers;
- The copyright of all material must be held by the school or be attributed to the owner where permission to reproduce has been obtained;
- Students will be taught to consider the thoughts and feelings of others when publishing material to websites and elsewhere. Material which victimises or bullies someone, or is otherwise offensive, is unacceptable and appropriate sanctions will be implemented.

Managing Teams

- All Staff and Students have access to Teams to use for professional and educational purposes;
- All staff must read and sign a copy of the Safe Working Practice Agreement Safeguarding Students and Young People and school's 'Acceptable Use of ICT Resources' document before being allowed controlled access to this service;
- All Students must read and sign a copy of the school's 'Acceptable Use of ICT Resources' document before being allowed controlled access to this service;
- Personal messaging between staff and students should not take place;
- Teams is managed centrally through Office 365 and all text conversations are recorded;
- Students' configured policies prevent them from directly messaging each other or messaging staff without staff first messaging them;
- All Teams meetings should be conducted professionally and where webcams are used backgrounds should be blurred, especially when meeting with external persons;
- Staff should avoid using the recording function when holding meetings;
- In cases where a meeting/training may need to be recorded, the staff member holding the meeting should acquire written consent from all members of the meeting;
- Staff should ensure that the sharing of images and videos does not breach image rights and copyrights. Seek permission from anyone included in personal photographs prior to sharing them;
- Students should avoid sending or sharing images or videos except when the media is a required piece of work;
- information shared within Teams is for use by the Teams members only and should not be shared outside of the Team without appropriate permissions. No Confidential, Personal or Sensitive information should be shared outside your Teams or the school;
- Students must not reveal details of themselves or others in any communication or by any personal web space such as an address, telephone number and must not arrange meetings with anyone;
- All conversations should be kept relevant to the particular chat or Team;
- Training on induction and Esafety training provide staff with continuous guidance;
- TJA reserves the right to remove inappropriate MS Teams sites or posts

Managing Information held

- The school conducts regular information audits to gain a clear and common understanding of the range of information assets it holds and those that are critical to business and ensure GDPR compliance.
- The school's information management of records policy offers further guidance on managing information
- Personal data sent over the network will be encrypted or otherwise secured.

Digital and video images

- When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Staff are allowed to take digital/video images, using school equipment, to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images.
- Care should be taken when taking digital / video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Students must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images.
- Students' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- The Jubilee Academy will not use publically or externally images of students whose parents or carers have not explicitly given their permission to do so.
- Staff must report any concerns relating to any inappropriate or intrusive photography to the Designated Safeguarding Lead.
- Staff must not use any images that are likely to cause distress, upset or embarrassment.
- Photographs taken by staff on school visits may be used in the curriculum and displayed within the school or at parents' evenings to illustrate the work of the school except in cases where the parent/carer has opted their child out.

Social networking and chat rooms

- The School will control access to moderated social networking sites and educate students in their safe use;
- Students will not access social networking sites e.g. 'Instagram', 'Facebook' or 'Twitter' on site;
- Students will be taught the importance of personal safety when using social networking sites, chat rooms and forums;
- Students will not be allowed to access public or unregulated chat rooms or forums;
- Students will only be allowed to use regulated educational chat environments and use will be supervised;
- Newsgroups will be blocked unless an educational need can be demonstrated;
- Students will be advised to use nick names and avatars when using social networking sites off site;
- Staff will not exchange social networking addresses or use social networking sites to communicate with students or parents;
- Should special circumstances arise where it is felt that communication of a personal nature between a member of staff and a pupil/parent is necessary, the agreement of a senior manager should always be sought first, and language should always be appropriate and professional.
- The School has a full Social media and networking policy that all staff must familiarize themselves with.

Mobile phones and electronic devices

- We advise against bringing mobile phones to school. All student mobile phones and other electronic devices are collected every morning and stored safely until end of day when they are returned to students
- The sending of abusive or inappropriate text messages or files by Bluetooth or any other means is forbidden and will be dealt with in accordance with the school's behaviour and preventing and responding to bullying policies;
- Students are not permitted to use the cameras in their mobile phones at any time;
- Staff will be issued with a school mobile phone where contact with students is necessary;
- iPads provided to staff must be used in accordance with the school Acceptable use policy both within school and outside;

- iPads provided to staff are done so to be used for work/educational purposes only and thus all apps installed should be appropriate for use in school;
- iPads for students should go through the school's web filtering so as to monitor use and help prevent students accessing inappropriate material;
- Where photos are to be taken of activities involving students a school issued technology should be used rather than personal technology;
- Staff will be issued with an iPad to support Teaching and Learning and/or duties associated with a staff member's job description.
- All Ipads are pass code protected and linked to an iCloud account tracking system in case of theft or loss

Cyber Security

This policy section outlines the school's guidelines and provisions for preserving the security of our data, technology infrastructure and systems to protect against malicious cyber-attacks/crime that can steal, damage or destroy information.

The more we rely on technology top collect, store and manage information the more vulnerable we become to sever data breaches. Human errors, hackers and system malfunctions could cause great financial damage and may jeopardise the school's reputation.

All staff must read and sign a copy of the Safe Working Practice Agreement Safeguarding Students and Young People and school's 'Acceptable Use of ICT Resources' document to confirm they have both read this policy and before being allowed controlled access to the ICT infrastructure.

For this reason, we have implemented the following security measures in accordance the DfE Cyber Security checklist for Academy Trusts
https://www.gov.uk/guidance/academies-guide-to-reducing-any-risk-of-financial-irregularities

The school will regularly review of this checklist and update this policy as required to ensure that the school has a clear understanding of cyber threats and vulnerabilities.

Authorising internet access

- All staff must read and sign a copy of the Safe Working Practice Agreement Safeguarding Students and Young People and school's 'Acceptable Use of ICT Resources' document before being allowed controlled access to this internet.
- Any staff not directly employed by the school will be asked to sign the school's 'Acceptable Use of ICT Resources' document before being allowed limited internet access from the school site;
- The School will maintain a current record of all staff and students who are allowed access to the school's ICT systems.
- The school will maintain a record of students whose parents/carers have specifically requested that their child be denied internet or e-mail access;
- Parents/carers will be asked to sign and return the school's form stating that they have read and understood the School's 'Acceptable Use' document and give permission for their child to access ICT resources;
- Staff will supervise access to the internet from the school site for all students.

User Education and awareness

It is essential that teachers and other adults working at the school are confident about using the internet in their work and should be given opportunities to discuss issues and develop appropriate teaching strategies.

All staff are governed by the terms of this policy and will be provided with a copy and its importance explained. All new staff will be given access to a copy of the policy during their induction.

Staff development in safe and responsible use of the internet and email will be provided as required. Staff will be aware that internet use will be monitored and traced to the original user. Discretion and professional

conduct is essential. Senior managers will supervise members of staff who operate the monitoring procedures.

Filtering, and monitoring systems

- The School will work in partnership with parents/carers, the DfE, partners and the Internet Service Provider to ensure appropriate filtering and systems are implemented to protect students and staff and that these are reviewed and improved regularly;
- These systems will ensure that there are effective anti-malware defenses in place across all business functions that have in built automatic scanning facilities at regular interval of the day such that any changes can be made as a result of monitoring results
- If staff or students discover unsuitable sites, the URL and content must be reported to the ICT Technician and Senior member of staff;
- Any material the School deems to be unsuitable or illegal will be immediately referred to the Internet Watch Foundation (www.iwf.org.uk);
- Regular checks by Senior Staff will ensure that the filtering methods selected are appropriate, effective and reasonable;
- Filtering methods will be age and curriculum appropriate.
- Filtering will provide a safe environment for students to learn in whilst also avoiding “over blocking”

Backups and Anti-Virus software

- All content that is saved to a shared or personal drive located on a server is backed up to a local server regularly;
- The local backup server regularly replicates backups to a secure datacenter hosted by European Electronique;
- All computers in the school have an anti-virus program (System Centre Endpoint Protection) with real time scanning installed to prevent any damage or data loss caused by malicious files or programs;
- The anti-virus software ensures that there are effective anti-malware defenses in place across all business functions that have in built automatic scanning facilities at regular interval of the day such that any changes can be made as a result of monitoring results

Removable media controls

- USB sticks and hard drives carry a huge risk of infection, so they should not be used on site at any time. If you feel there is an extreme circumstance in which a USB needs to be used you need to speak with ICT to have it scanned and approved before EVERY use, even if it has been scanned multiple times before.

Information risk management regime

Emerging technologies offer the potential to develop teaching and learning tools but need to be evaluated to assess risks, establish the benefits and to develop good practice. The senior leadership team should be aware that technologies such as mobile phones with wireless internet access can bypass school filtering systems and allow a new route to undesirable material and communications.

In common with other media such as magazines, books and video, some material available through the Internet is unsuitable for students. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to international scale and linked nature of Internet content, it is not always possible to guarantee that unsuitable material may never appear on a school computer. The school cannot accept liability for the material accessed, or any consequences of Internet access.

- The school has an Esafety risk assessment to identify, assess and minimise risks, which is reviewed regularly by senior management representation and safeguarding governor to ensure appropriate governance engaged with risk mitigation processes. This then feeds into the Esafety staff training programme to cover secure use of systems.
- A Data Protection Impact Assessment (DPIA) will be conducted by the Data Protection Officer on any new emerging technologies that are likely to result in a high risk to individuals.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Criminal Misuse Act 1990 and will be dealt with accordingly.

The “Three C’s” (Content, Contact and Conduct) will be employed to determine and minimize risks associated with use of technologies with online access.

	Commercial	Aggressive	Sexual	Values
Content (child as recipient)	Adverts Spam Sponsorship Personal info	Violent/hateful Content	Pornographic or unwelcome sexual content	Bias Racist Misleading info or advice
Contact (child as participant)	Tracking Harvesting personal info	Being Bullied, harassed or stalked	Meeting strangers Being groomed	Self-harm Unwelcome persuasions
Conduct (child as actor)	Illegal downloading Hacking Gambling Financial scams Terrorism	Bullying or harassing another	Creating and uploading inappropriate material	Providing misleading info/advice

- The Head of School will ensure that the E-Safety Policy is implemented and compliance with the policy is monitored. Access to any websites involving gambling, games or financial scams is strictly forbidden and will be dealt with accordingly.
- Rules for Internet access will be posted in all rooms where computers are used.
- Responsible Internet use, covering both school and home use, will be included in the SMSC curriculum. Students will be instructed in responsible and safe use before being allowed access to the Internet and will be reminded of the rules and risks before any lesson using the Internet.
- Students will be informed that internet use will be closely monitored, and that misuse will be dealt with appropriately.

Maintaining user privileges

The school has effective account management processes with limited on privileged accounts that are monitored and controlled by the School Business Manager in partnership with the ICT Technician.

Users will be given appropriate and controlled access both data and administrative controls as is deemed necessary for them to conduct their job specific duties, based on their potential needs and risks of misuse.

Locks are in place on user accounts after multiple failed attempts to login to account and automatic lock outs of accounts when not in use for a specified time

Secure Configuration and Password Security

The school has a system inventory. All devices require a password/ pass code protection. Computers are set up from one defined image with security features preinstalled. This allows for automatic security patches to be applied

Password security is a crucial part of e-Safety. In order to make sure a high level of password security is attained; The Jubilee Academy enforces a set of complexity requirements and rules that are set via group policy.

These requirements state and enforce that passwords must:

- Not contain the user's account name or parts of the user's full name that exceed two consecutive characters
- Be at least seven characters in length
- Contain characters from three of the following four categories:
    - English uppercase characters (A through Z)
    - English lowercase characters (a through z)
    - Base 10 digits (0 through 9)
    - Non-alphabetic characters (for example, $, #, %)
- Be changed every 90 days

Reporting and Recording Misuse

The Jubilee Academy has a clear process for reporting misuse of the school's ICT. In the case of an incident any witnesses are to report the incident to the e-safety lead and the ICT Technician. An Esafety form will need to be filled out and statements will be taken. Appropriate action and sanctions, if any, will then be taken/enacted.

Once a report is completed it will be logged anonymously in the TJA e-Safety Concern Log and any changes that are implemented as a result of the incident will also be noted.

Unapproved system utilities and executable files will not be allowed in students' work areas or attached to e- mails. The ICT technician will ensure that the system has the capacity to deal with increased traffic caused by Internet use.

Parents/carers and students will work in partnership with the school staff to resolve any issues. As with issues to do with substance misuse, there may be occasions when the school must contact the police. If appropriate, early contact should be made to discuss strategies and preserve possible evidence.

Sanctions for misuse may include any or all of the following:

- Interview/counseling by an appropriate member of staff;
- Informing parents/carers;
- Removal of internet access for a specified period of time, which may ultimately prevent access to files held on the system, including examination coursework;
- Exclusion;
- Referral to the police.

Incident management

The School's Business Continuity plan provides an incident and response disaster recovery capability with suitably trained staff

There are incident response management plans are in place in the event of any threat for critical ICT system and services for the school including fraud, which are tested annually on a rolling basis.

Network Security

The School works in partnership the Internet Service Provider to ensure the network perimeter is managed with robust filter controls

This is tested by regular use which monitored and reported in case of an incident that can be rectified immediately to ensure the network is completely protected against any threats.

Home and mobile working

Risks Associated with Remote Access

As with all use of technology, there are risks associated with the use of remote access. These risks include but are not limited to:

- Damage or loss of equipment
- Loss of data
- Misuse of data or information – both intentional and unintentional
- Theft of data or information – both intentional and unintentional
- Potential legal action against the School or individuals as a result of information loss or misuse.
- Potential sanctions against the School or individuals imposed by the Information Commissioner's Office as a result of information loss or misuse.
- Unauthorised access to confidential information
- Virus or malware infection

Responsibilities of Staff

When using remote access, staff MUST follow these guidelines:

- Staff must not use public computers for remote access and should only use their own personal equipment or school provided equipment
- Staff must only use remote access when in a safe and secure environment
- Staff must never leave a device unattended whilst logged into remote access
- Staff must always log out of remote access when finished or when taking an extended break.
- Staff are expected to act as they would on school grounds: remote access is a professional environment and staff should conduct themselves as such when logged on.
- Staff must keep their passwords secure. Passwords must never be given out to someone else (whether employed by TJA or not) and nobody but the person signed in should use remote access
- Passwords should be memorable enough that they do not need to be written down(as this is prohibited) but also secure enough that nobody could guess it
- Staff must never use remote access when logged in as somebody else
- Staff must always make sure the device being used to connect to remote access has an up to date anti-virus to protect the school system from infection.
- Do not install programs on the remote desktop, if you need a program installed please speak to ICT
- Staff must not download confidential information from the school systems via remote access to a personal device or to any device other than school issued equipment
- Staff must always adhere to the E Safety and Acceptable Use of ICT Policy when using remote access.
- Staff will receive training and guidance on best practice when using remote access and be required to sign to agree to abide by the guidelines to use the remote access system responsibly and for work purposes only

Mobile Devices – School tablets and laptops

1. What strategies are there in place for preventing damage, theft and loss?

All mobile devices

- Marked as TJA property with security sticker.
- When purchased they are added to a spreadsheet inventory which lists all the devices owned by the school, who has possession of those devices, their ID number and the Serial Number of the device.
- A check is done on every device each time it is given out and upon return. When students use laptops, the staff member supervising is given a sheet which details any prior damage and leaves room for the recording of names of students who use each laptop.
- Clear guidelines are given to staff half termly in regards to the booking, monitoring and care of mobile devices.

Students

- All tablets are given to students in a protective hard book covering to protect the tablet when in use.
- All students and their parents sign an acceptable use before they are given a tablet or a laptop to use. This contract explains how students need to look after the tablet and their liability should the tablet be damaged.
- On receiving their device all students are given training on how to maintain and look after their tablet.

Staff

- All Staff tablets are given in a protective case; laptops, when taken off site, are given in a protective bag.
- All Staff sign the ICT Acceptable agreement when they are given a tablet or laptop which explains what they need to do to look after their device.

2. What strategies are in place for monitoring the condition of the mobile devices?

- The finance department carries out a regular audit of the staff devices and asks a sample of staff to bring in their device so that they can be checked.

3. What happens if a mobile device is lost or damaged

Students

- Parents are informed via a phone call and a letter.
- If a device requires a replacement part due to damage caused when in the child's care parents are charged the cost to replace the part (Exceptions may be given based on the financial situation of the family involved)
- If a device is damaged beyond repair or is lost when in the child's care parents are charged the cost to replace the device (Exceptions may be given based on the financial situation of the family involved

Staff

- The Head of Department is informed.
- Payment of the insurance excess is taken from the departmental budget.

4. What happens if a mobile device is accidentally damaged or not working

Students

- Staff notify the IT technician via email and on any sheets provided with the device. The device is checked, then if damaged/broken, logged on the inventory as damaged/broken
- IT will attempt to fix the device
- If the tablet cannot be repaired by the IT technician, parents are informed via a phone call and a letter
- Parents are asked to contribute £20 toward the insurance excess.
- Finance are informed and a payment option is set up.

Staff

- Staff take the device to the IT technician who will attempt to repair.
- If the device cannot be repaired by the IT technician, the Head of Department is informed and the insurance excess is taken from the staff/departmental budget.

Monitoring, evaluation and review

The effectiveness of this policy is regularly monitored through the school's self-evaluation schedule.

E-safety incident report form

This form should be kept on file and a copy emailed to The Jubilee Academy's e-safety officer at m.boothe@thejubileeacademy.org.uk and a.goodenough@thejubileeacademy.org.uk

Details of incident

Date happened:_____**Date reported:** _____

Time happened: _____

Name of person reporting incident: _____

If not reported, how was the incident identified? _____

Where did the incident occur?
□ In school setting □ Outside school setting

Who was involved in the incident?
□ child/young person □ staff member □ other (please specify

Type of incident:
□ bullying or harassment (cyber bullying
□ deliberately bypassing security or access
□ hacking or virus propagation
□ racist, sexist, homophobic religious hate material
□ terrorist material
□ drug/bomb making material
□ child abuse images
□ on-line gambling
□ pornographic material
□ illegal pornographic material
□ other (please specify) _____

Nature of incident

□ **Deliberate access**

Did the incident involve material being;
□ created □ viewed □ printed □ shown to others
□ transmitted to others □ distributed

Could the incident be considered as;
□ harassment □ grooming □ cyber bullying □ breach of AUP

□ **Accidental access**

Did the incident involve material being;
□ created □ viewed □ printed □ shown to others
□ transmitted to others □ distributed

Description of incident

Action taken

Reporting Staff Member

□ Incident reported to ICT
□ Incident reported E-safety Coordinator
□ Behaviour Point logged on SIMS
□ Device confiscated from student
□ Student removed from classroom/away from equipment

ICT

□ Impero/Lightspeed logs acquired
□ Student access blocked pending investigation
□ Incident reported to E-safety Coordinator
□ Incident reported to social networking site
□ Impero/Lightspeed filtering updated
□ ICT AUP to be reviewed/amended/updated
□ E-safety Incident Log Updated
□ e-safety policy to be reviewed/amended/updated
□ Behaviour Point logged on SIMS (if not done by reporting staff member)

E-Safety Coordinator/SLT

□ Statements Gathered
□ Advice sought from Safeguarding and Social Care
□ Referral made to Safeguarding and Social Care
□ Incident reported to social networking site
□ incident reported to police
□ Child's parents informed
□ Disciplinary action to be taken
□ Child/young person debriefed

Outcome of incident/investigation