James Brindley

Digital Citizenship & E-Safety Policy

Agreed by SLT: November 2020
Review: November 2023
Signed by:

Content

Background and Rationale

At James Brindley Academy, we understand that computer technology is an essential resource for supporting teaching and learning. The internet, and other digital and information technologies, open opportunities for young people and play an important role in their everyday lives.

Whilst the Academy recognises the importance of promoting the use of computer technology throughout the curriculum, we also understand the need for safe internet access and appropriate use, especially for young people who are at increased risk due to SEMH.

Our Academy has created this policy with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all young people and staff. The Academy is committed to providing a safe learning and teaching environment for all and has implemented important controls to mitigate the risk of harm. This policy links

ICT, safeguarding and other policies and procedures to reflect the how the Academy deals with e-safety issues and supports us to become effective digital citizens in a connected world.

> ***Article 30*** *Every child has the right to learn and use the language, customs and religion of their family, regardless of whether these are shared by the majority of the people in the country where they live.*

Think Differently

This policy supports our Vision by working towards the following Missions:

- Mission 1: Delivering a pupil-centred, holistic curriculum which prepares young people to overcome barriers for life.
- Mission 2: Ensuring that all pupils and staff are safe by leading a transparent and ethically driven organisation
- Mission 4: Creating an innovative, optimistic, and skilled workforce

Development/Monitoring and Review

The documents referred to in this Digital Citizenship & E-safety Policy have been developed by various groups/individuals:

- Principal/Senior Leaders/Designated Safeguarding Leads (DSL)
- Teachers
- Support Staff
- ICT Technical staff
- Trustees
- Parents and Carers
- Young people

The Digital Citizenship & E-Safety Policy will be reviewed every 3 years, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place. Other associated policies that should be read in conjunction with this policy are listed at the end of the policy. Should serious e-safety incidents take place, the following persons/agencies should be informed: Lead DSL, LADO, Police Commissioner's Office. The Academy will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited) using software such as Impero or SENSO
- Internal monitoring data for network activity

- Surveys/questionnaires of young people, parents/carers and staff

Scope of the Policy

This policy applies to all members of the Academy community (including staff, agency staff, young people, volunteers, parents/carers, visitors and community users) who have access to and are users of Academy ICT systems, both in and out of Academy.

The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of young people when they are off the Academy site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place out of Academy, but is linked to membership of the Academy. The Academy will deal with such incidents within this policy and associated behaviour and antibullying policies and will, where known, inform parents/carers of incidents of inappropriate e-safety behaviour that take place out of Academy.

Legal framework

This policy has due regard to all relevant legislation including, but not limited to:

- The General Data Protection Regulation 2018
- Freedom of Information Act 2000

This policy also has regard to the following statutory guidance:

- DfE (2020) 'Keeping children safe in education'
- National Cyber Security Centre (2017) 'Cyber Security: Small & Medium Business

This policy will be used in conjunction with the following Academy policies and procedures:

1. Anti-Bullying & Anti-Harassment Policies
2. Child Protection Policy
3. Data Protection Policy
4. Acceptable Use of Technology Agreement

Article 8 *(protection and preservation of identity) Every child has the right to an identity. Governments must respect and protect that right, and prevent the child's name, nationality or family relationships being changed unlawfully*

Article 28 *(right to education) Every child has the right to an education. Primary education must be free and different forms of secondary education must be available to every child. Discipline in schools must respect children's dignity and their rights. Richer countries must help poorer countries achieve this.*

Roles and responsibilities

Principal & Senior Leadership Team

- The Principal will review and amend this policy with SLT and Data Protection Officer (DPO), considering new legislation, government guidance and previously reported incidents, to improve procedures.
- The Principal is responsible for ensuring that relevant staff receive CPD. SLT will provide all relevant training and advice for members of staff as part of the updated safeguarding training and be able to teach young people about online safety. The Academy will regularly educate staff, young people and parents on the skills needed to live in a digital world.

- The Principal will establish a procedure for reporting incidents and inappropriate internet use, either by young people or staff.
- The Principal is responsible for communicating with parents regularly and updating them on current e-safety issues and control measures.
- The Principal will be responsible for the overall content of the website and will ensure the content is appropriate and accurate.
- The Assistant Principal for Teaching & Learning (T&L) & Assistant Principal for Safeguarding and Inclusion, are responsible for ensuring the day-to-day e-safety in the Academy and managing any issues that may arise.
- The Assistant Principal for T&L, Data Protection Officer (DPO) and IT Manager will ensure there is a system in place for monitoring e-safety in the Academy, keeping in mind data protection requirements.
- The Assistant Principal for T&L & Assistant Principal for Safeguarding and Inclusion will monitor the provision of e-safety in the Academy and will provide feedback to the Principal.
- SLT will ensure that all members of staff are aware of the procedure when reporting e-safety incidents and will keep a log of all incidents recorded.
- SLT will feedback to the Board of Trustees on the effectiveness of the e-safety provision, current issues, and to review incident logs, as part of the Academy's duty of care. The SLT will evaluate and review this Digital Citizenship & E-safety Policy on an annual basis, considering the latest developments in ICT and the feedback from staff/young people.
- The SLT will complete an annual review of online safety and use recommendations to update this policy and practice.

IT Department (Technical)

- IT Department are responsible for ensuring that there are appropriate filtering and monitoring systems are in place to safeguard all IT users. The system should not lead to 'over blocking' – unreasonable restrictions as to what young people can be taught with regards to online teaching and safeguarding.
- IT Department will ensure all Academy systems will be protected by up-to-date virus software.
- Firewalls will always be switched on – IT Department will review these on a weekly basis to ensure they are running correctly and to carry out any required updates.
- Firewalls and other virus management systems, e.g. anti-virus software, will always be maintained by the IT Department.
- IT Department is responsible for ensuring that all Academy-owned devices are password protected – these passwords will be changed between users to ensure their security.
- IT Department is responsible for all mobile devices being fitted with tracking software to ensure they can be retrieved if lost or stolen. To protect, retrieve and erase personal data, all mobile devices and hand-held computers will be fitted with software to ensure they can be remotely accessed.
- IT Department will review all mobile devices on a termly basis to ensure all apps are compliant with data protection regulations and up-to-date, and to carry out any required updates.
- IT Department and a member of the wider leadership team will review and authorise any apps and/or computer programmes before they are downloaded.
- The IT Department will ensure all Academy-owned laptops and computers have their encryption settings turned on or, if there is no built-in encryption option, encryption software is installed.

- IT Department will provide guidance on setting and managing passwords including managing the length of time users have the same password.
- Technical security features, such as virus software, are kept up-to-date and managed by the IT Department.
- IT Department will ensure that the filtering of websites and downloads is up-to-date and monitored.

All Staff

- It is the responsibility of all staff to be alert to the possible harm that young people or staff can suffer due to inappropriate hardware, software, internet access or use, both inside and outside of the Academy, and to deal with incidents of such as a priority.
- Staff are responsible for ensuring that e-safety issues are embedded in the curriculum and safe internet access is always promoted.
- All staff are responsible for ensuring they are up to date with current e-safety issues, and this Digital Citizenship & E-safety Policy.
- All staff and young people will ensure they understand and adhere to our Acceptable Use of Technology Agreement, which they must sign.
- Staff are permitted to use the technology for personal use during out-of-Academy hours, as well as break and lunch times. Personal use will only be monitored by SLT for access to any inappropriate or explicit sites, where the need to do so outweighs the need for privacy. Inappropriate internet access by staff may result in the staff member being permitted to use the internet for Academy purposes only and prohibited from using any personal devices. This will be dealt with following the process outlined in the misuse by staff section of this policy.
- Staff are not permitted to communicate with young people over personal social networking sites or use any personal email accounts and are reminded to set their privacy settings accordingly, to minimise public scrutiny.
- Staff are not permitted to publish comments which may negatively affect the Academy's reputation negatively.
- Staff are able to take pictures, though they must do so in accordance with our Permissions Letter & Privacy Notice.
- Staff will not take pictures using their personal equipment.
- Any member of staff that is representing the Academy online, e.g. through blogging, must express neutral opinions and not disclose any confidential information regarding the Academy, or any information that may affect its reputability.
- Staff using personal data, e.g. those including pupils' medical records, should store this information securely in the following locations:
    - Pupil information in Arbor
    - Safeguarding, including child protection, information in CPOMS
    - Staff information in Arbor
- Where it is part of an individual's job sharing of personal data with relevant people will be done via encrypted software.
- Staff members will report all malware and virus attacks to the IT Department and DPO immediately.
- Staff will not view or forward illegal images of a child. If they are made aware of such an image, they will contact the DSL.
- Staff should report any inappropriate use of social media by a colleague through the Whistleblowing Policy.

Centre Leaders

- Centre Leaders will share E-safety information with parents through a variety of formats; paper, presentation, courses and online formats.
- Centre Leaders will, at the start of each Academy year, hold an assembly explaining e-safety information to Young People. They will explain that monitoring and filtering systems will detect inappropriate links, viruses, malware and profanity and that the young people should support the academy by reporting any undetected items.
- Academy Leaders will support staff in becoming effective digital citizens.

Personal Development Teachers

- Young people will be educated about online safety through teaching and learning opportunities as part of a broad and balanced curriculum; this includes covering relevant issues within PD lessons as well as sex and relationship education. Coverages will be categorised into three areas of risk:
    - **content**: being exposed to illegal, inappropriate or harmful material; for example pornography, fake news, racist or radical and extremist views;
    - **contact**: being subjected to harmful online interaction with other users; for example commercial advertising as well as adults posing as children or young adults; and
    - **conduct**: personal online behaviour that increases the likelihood of, or causes, harm; for example making, sending and receiving explicit images, or online bullying.
- Personal Development teachers will deliver a Personal Development Curriculum that will include E-Safety and preparing Young People to be digitally safe and literate. Guidance by Living in a connected world, CEOP, UKCCIS - and supported by a variety of resources including: Common Sense recommended by SWGFL and SaferInternet / Be Internet Legends from Google / https://projectevolve.co.uk/

> ***Article 34*** *(sexual exploitation) Governments must protect children from all forms of sexual abuse and exploitation.*
> ***Article 19*** *(protection from violence, abuse and neglect) Governments must do all they can to ensure that children are protected from all forms of violence, abuse, neglect and bad treatment by their parents or anyone else who looks after them.*

Young People

- All young people are aware of their responsibilities regarding the use of Academy-based ICT systems and equipment, including their expected behaviour.
- Young people may only use approved e-mail accounts on the Academy system.
- Young people must immediately tell a member of staff if they receive an offensive e-mail/message.
- Young people must not reveal details of themselves or others in e-mail communication, such as address or telephone number, or arrange to meet anyone.
- Young people should take a screen shot to evidence any inappropriate or offensive comments and inform the DSL immediately. The screen shot should not be shared.
- Young people are not permitted to take or publish photos of others.
- Any inappropriate or offensive comment to, or about, another young person in Academy will be treated in line with the Academy's Positive Behaviour Policy.
- Young people will not open any email or attachment that is from someone they do not already know without the permission of Academy staff.

- Young people are not permitted to access the Academy's Wi-Fi system at any time using their personal mobile devices.
- Any young person who does not adhere to the rules outlined in our Acceptable Use of Technology Agreement and is found to be wilfully misusing technology will be treated in line with the Academy's Positive Behaviour Policy.

Parents/Carers

- Parents/carers are responsible for ensuring their child understands how to use computer technology and other digital devices appropriately.
- Permission to use a child's photograph will be obtained from parents/carers prior to its use.

Technology Guidance

Email

- Young people and staff will be given approved email accounts for education and academy use, private accounts should be used for personal business and socialising. Pupil email accounts may be withdrawn by the Centre Leaders if the young person is considered to be a risk. Centres must carry out a risk assessment prior to this request.
- Whole-class or group e-mail addresses should be used at Key Stage 2 and below.
- The use of personal email accounts for academy work is prohibited.
- No sensitive personal data shall be sent to third parties via email unless using encryption and/or? password protection.
- Any emails sent by young people to external organisations will be overseen by their class teacher and must be authorised before sending.
- Chain letters, spam and all other emails from unknown sources must be deleted without opening.
- Staff will not be sanctioned if they are caught out by cyber-attacks as this may prevent similar reports in the future. A member of the SLT will investigate; however, this will be to identify the cause of the attack, any compromised data and if there are any steps that can be taken in the future to prevent similar attacks happening.

Social networking

- The use of social media on behalf of the Academy will be conducted through the Leadership Communications Officer, in line with GDPR and communication guidelines.
- Access to social networking sites will be filtered as appropriate.
- Should access be needed to social networking sites for any reason, this will always be monitored and controlled by staff and must be first authorised by a member of SLT.
- Social networking, e.g. Facebook/Twitter/MSN sites should not be accessed during Academy hours, unless agreed by a member of SLT and is for a legitimate educational purpose. Some of our young people are not legally old enough to use these, i.e. Facebook has an age restriction of 13.

Published content on the Academy website

- Contact details on the Academy website will include the phone number, email and address of the Academy. Names and photographs of staff, trustees and young people will only be published with explicit permission, no other personal information will be shared.
- The point of contact on the website will be the Academy address, Academy e-mail and telephone number. Staff or pupils' home information will not be published.
- Pupils' full names will not be used anywhere on the website.

- Written consent from parents/carers will be obtained prior to pupil photographs being published on the academy website.

System Security

- Each person is responsible for their individual use. If you are away from your computer, you are expected to lock it.
- Each person must not give account or password information to another user or allow another user to utilise their account.
- Users will immediately notify someone if a possible security problem is identified. Do not go looking for security problems because this may be construed as an illegal attempt to gain access.
- If the IT department need to access your screen, they will ask the user to confirm that no personal data is viewable.

Devices

- Apps will only be downloaded from manufacturer approved stores, e.g. Google Play and the Apple App Store.
- Young people at Ardenleigh will only have access to PCs.

Internet

- Any requests by staff for websites to be added or removed from the filtering list must be authorised by a member of SLT.
- The Academy will keep a record of any young people whose parents have specifically denied them internet or e-mail access.
- At Key Stage 1, access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials.
- At Key Stage 2 parents will be informed that young people will be provided with supervised Internet access.
- Secondary - By using the Internet, secondary young people are agreeing to abide by the Acceptable Use of Technology Agreement.

Cyber bullying

- For the purposes of this policy, cyber bullying is a form of bullying whereby an individual is the victim of harmful or offensive messages, or the posting of information or images online. The Academy recognises that both staff and young people may experience cyber bullying and is committed to responding appropriately to instances that should occur. The Academy will commit to creating a learning and teaching environment which is free from harassment and bullying, ensuring the happiness of all members of staff and young people.
- The Academy has zero tolerance for cyber bullying, and any incidents will be treated with the utmost seriousness and will be dealt with in accordance with our Anti-Bullying and Harassment Policy.
- The Principal will decide whether it is appropriate to notify the police.

Misuse by young people

- Any instances of misuse should be immediately reported to a member of staff, who will then report this to the SLT.

Misuse by staff

- Any misuse of the internet by a member of staff should be immediately reported follow the whistleblowing policy. The Principal will deal with such incidents in accordance with the Disciplinary Policy and may decide to take action against the member of staff. The Principal will decide whether it is appropriate to notify the police and/or LADO of the action taken against a member of staff.

Use of illegal material

- In the event that illegal material is found on the Academy's network, or evidence suggests that illegal material has been accessed, the police will be contacted.
- Incidents will be immediately reported to the Internet Watch Foundation and the police will be contacted if the illegal material is, or is suspected to be, a child sexual abuse image hosted anywhere in the world, a non-photographic child sexual abuse image hosted in the UK, or criminally obscene adult content hosted in the UK.
- If a child protection incident is suspected, the Academy's child protection procedure will be followed – the DSL and Principal will be informed, and the police contacted.

James Brindley Academy
Acceptable Use of Technology Agreement (Pupil)

Pupils' Name	
Centre	

When using the Academy's ICT facilities and accessing the internet in school, I will not:

- Use them for a non-educational purpose
- Use them without a teacher being present, or without a teacher's permission
- Use them to break school rules
- Access any inappropriate websites
- Reveal details of myself or others in e-mail communication or online, such as address or telephone number, or arrange to meet anyone.
- Take or publish photos of others
- Access social networking sites (unless my teacher has expressly allowed this as part of a learning activity)
- Use chat rooms, chain letters or spam.
- Open any attachments in emails, or follow any links in emails, without first checking with a teacher.
- Use any inappropriate language when communicating online, including in emails.
- Share my password with others or log in to the school's network using someone else's details.
- Access the Academy's Wi-Fi system at any time using my personal mobile devices.
- Bully other people.

- I will always use the Academy's ICT systems and internet responsibly by:
- Only using approved e-mail accounts on the Academy system.
- Immediately telling a member of staff if I receive an offensive e-mail/message.
- Immediately letting a teacher or other member of staff know if I find any material which might upset, distress or harm me or others.
- Taking a screen shot to evidence any inappropriate or offensive comments and inform the DSL immediately. I will not share the screen shot.
- Not installing or downloading any software or programs or alter the Academy's software in any way. This includes transferring data from home to Academy.

I understand that:

- Any inappropriate or offensive comment to, or about, another young person in Academy will be treated in line with the Academy's Positive Behaviour Policy.
- Any inappropriate use of IT will be dealt with in line with the Academy's Positive Behaviour Policy.
- The Academy will monitor the websites I visit and my use of the school's ICT facilities and systems.

Pupil's Signature	
Date	

Sites you might find useful:

- Childline for free and confidential advice
- UK Safer Internet Centre to report and remove harmful online content
- CEOP for advice on making a report about online abuse

James Brindley Academy
Acceptable Use of Technology Agreement (Parents/Carer)

I understand that I am responsible for ensuring my child understands how to use computer technology and other digital devices appropriately.

The Academy will use the following channels:

- Email/text groups for parents (for school announcements and information)
- Arbor App
- Our official social media accounts
- Academy Website

When communicating with the Academy via official communication channels, or using private/independent channels to talk about the school, I will:

- Be respectful towards members of staff, and the school
- Be respectful of others
- Direct any complaints or concerns through the school's official channels, so they can be dealt with in line with the school's complaints procedure.

I will not:

- Use private groups, the Academy's Facebook page, or personal social media to complain about or criticise members of staff.
- Use private groups, the Academy's Facebook page, or personal social media to complain about, or try to resolve, a behaviour issue involving other pupils. I will contact the school 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 other children's parents/carers

- I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the Academy's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.

Parent/Carer's Name	
Parent/Carer's Signature	
Date of Signature	

As a parent you can use the following to support your child:

- Childnet offers a toolkit to support parents and carers of children of any age to start discussions about their online life, to set boundaries around online behaviour and technology use, and to find out where to get more help and support
- Commonsensemedia provide independent reviews, age ratings, & other information about all types of media for children and their parents
- Government advice about protecting children from specific online harms such as child sexual abuse, sexting, and cyberbullying
- Government advice about security and privacy settings, blocking unsuitable content, and parental controls
- Internet Matters provide age-specific online safety checklists, guides on how to set parental controls on a range of devices, and a host of practical tips to help children get the most out of their digital world
- Let's Talk About It provides advice for parents and carers to keep children safe from online radicalisation
- London Grid for Learning provides support for parents and carers to keep their children safe online, including tips to keep primary aged children safe online
- Lucy Faithfull Foundation StopItNow resource can be used by parents and carers who are concerned about someone's behaviour, including children who may be displaying concerning sexual behaviour (not just about online)
- National Crime Agency/CEOP Thinkuknow provides support for parents and carers to keep their children safe online
- Net-aware provides support for parents and carers from the NSPCC and O2, including a guide to social networks, apps and games
- Parentzone provides help for parents and carers on how to keep their children safe online
- Parent info from Parentzone and the National Crime Agency provides support and guidance for parents from leading experts and organisations
- UK Safer Internet Centre provide tips, advice, guides and other resources to help keep children safe online

James Brindley Academy
Acceptable Use of Technology Agreement (Staff)

I will always use the Academy's ICT systems and internet responsibly by:

- being alert to possible harm to young people or staff due to inappropriate hardware, software, internet access or use, both inside and outside of the Academy, and to deal with incidents of such as a priority.
- ensuring that e-safety issues are embedded in the curriculum and safe internet access is always promoted.
- keeping up to date with current e-safety issues, and this Digital Citizenship & E-safety Policy.
- only using technology for personal use during out-of-Academy hours, including break and lunch times.
- altering my privacy settings to ensure data is private.
- taking pictures, relevant to work, in accordance with the Permissions Letter & Privacy Notice.
- expressing neutral opinions and not disclosing any confidential information regarding the Academy, or any information that may affect its reputation when representing the Academy on-line, such as through blogging.
- storing sensitive information securely in the following locations:
    - Pupil information in Arbor
    - Safeguarding, including child protection, information in CPOMS
    - Staff information in Arbor
- using encrypted software or password protecting documents when sharing sensitive data
- reporting malware and virus attacks to the IT Department and DPO immediately.
- reporting any inappropriate use of social media by a colleague to the Principal or through the Whistleblowing Policy.
- taking all reasonable steps to ensure that work devices are secure and password-protected when using them outside school,
- keeping all data securely stored in accordance with this policy and the school's Data Protection Policy.
- letting the designated safeguarding lead (DSL) and ICT manager know if a pupil 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.
- always using the school's ICT systems and internet responsibly and ensuring that pupils in my care do so too.

When using the Academy's ICT facilities and accessing the internet in school, or outside school 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)
- communicate with young people over personal social networking sites or personal email accounts
- use them in any way which could harm the school'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 the school's network
- share my password with others or log in to the school's network using someone else's details
- share confidential information about the school, its pupils or staff, or other members of the community
- access, modify or share data I am not authorised to access, modify or share
- promote private businesses unless that business is directly related to the school.

Staff Name		Staff's Signature	
Date of Signature			

You may find the following helpful:

- Childnet provide guidance for schools on cyberbullying
- Educateagainsthate provides practical advice and support on protecting children from extremism and radicalisation
- London Grid for Learning provides advice on all aspects of a school or college's online safety arrangements
- NSPCC provides advice on all aspects of a school or college's online safety arrangements
- Safer recruitment consortium "guidance for safe working practice", which may help ensure staff behaviour policies are robust and effective
- Searching screening and confiscation is departmental advice for schools on searching children and confiscating items such as mobile phones
- South West Grid for Learning provides advice on all aspects of a school or college's online safety arrangements
- Use of social media for online radicalisation - A briefing note for schools on how social media is used to encourage travel to Syria and Iraq.
- UK Council for Internet Safety have provided advice on sexting-in-schools-and colleges and using-external-visitors-to-support-online-safety-education

Remote education, virtual lessons and live streaming

- Case studies on remote education practice are available for schools to learn from each other
- Departmental guidance on safeguarding and remote education including planning remote education strategies and teaching remotely
- London Grid for Learning guidance, including platform specific advice
- National cyber security centre guidance on choosing, configuring and deploying video conferencing
- National cyber security centre guidance on how to set up and use video conferencing
- UK Safer Internet Centre guidance on safe remote learning

LOAN AGREEMENT

1. All equipment is loaned to you by the Academy on a temporary basis only.
2. The loan agreement exists between the Academy and the above-named person.
3. Equipment will be loaned to the named person whilst in employment and must be returned if the employment ceases, or at any time requested to be returned.
4. All loaned equipment and associated peripherals remain the property of James Brindley.
5. All ICT loaned equipment will come with any required software pre-installed. An ICT technician must carry out all software installations. At no point must you attempt to make any changes to equipment hardware.
6. Any ICT equipment including connectivity equipment must not be used for any illegal and/or antisocial purpose, in accordance with the Digital Citizen Policy.
7. Mobile phones may be used for personal use. This must be pre-agreed when issued and you will be charged £10 per month towards the cost of the usage.
8. The use of all equipment will comply with all relevant GDPR legislation, personal data should not be stored on any James Brindley owned equipment.
9. If any equipment is stolen you must immediately report it to the police and get a crime reference number, and immediately report this to your line manager.
10. You must not remove any labels that are attached to the equipment, including but not limited to, asset labels and PAT testing labels.
11. Reasonable health and safety precautions should be taken when using equipment. The school is not responsible for any damage to person or property resulting from the misuse of equipment.
12. You have a responsibility to take reasonable care to ensure the security of all loaned equipment.
13. James Brindley reserves the right to charge the replacement cost of loaned equipment to the borrower should the equipment not be returned, or in the condition which it was issued. In consideration of loaning the Equipment, you agree that if James Brindley incurs any cost in relation to loss or damage, or if your employment terminates after we have incurred liability for the cost, you will be liable to repay all of the fees, expenses and other costs associated with such loss or damage in accordance with the following;
    You shall repay us as follows:
    - if you cease employment and fail to return the Device loaned to you within 5 working days the full costs of replacement shall be repaid;
    - if you destroy or damage the Device either intentionally or accidentally, whether externally or internally, the full cost of repairs or replacement shall be repaid;
    - if you lose or fail to return the Device, whether by reason of theft or otherwise, within 5 working days the full costs of replacement shall be repaid;

    You agree to us deducting the sums under this clause from your salary, final salary or any outstanding payments due to you.
14. Any breach of this agreement whether deliberate or otherwise could result in the initiation of disciplinary action against you.
15. Equipment will only be loaned when this agreement has been completed and signed.

LOANED ITEM DETAILS

ICT Equipment

Date of Loan:	
Item Loaned:	
Reference No:	
Details of Additional Items:	

Mobile Phone

Date of Loan:	
Model:	
Telephone Number:	
Will this be used for personal use?	YES / NO If yes, I agree to a termly invoice of £10 as a personal contribution

Lone Worker Device

Date of Loan:	
Device No/Ref:	

Other Items

Date of Loan:	
Item Loaned:	

I, …..……..…...have read the above agreement and its terms and agree to reimburse and remedy James Brindley Academy if I breach the above conditions of loan. I also give consent to James Brindley Academy to deduct from my salary any sums/payments that become due under this agreement.

Signature of Borrower: Date:

Name of Issuer:
Signature of Issuer: Date:

This will be in an electronic format.