**Harrison College Ltd**

# IT Acceptable Usage Policy

# (including Remote Learning/Offsite Provision)

Review date: February 2024
BoD Approval: February 2024
Next Review: September 2024

**Purpose**

The purpose of this policy is to define standards, procedures, and restrictions for staff members and students who have legitimate business requirements to use a private or College-provided mobile device that can access the College's electronic resources. This mobile device policy applies to, but is not limited to, all devices and accompanying media that fit the following device classifications:

- Laptop/notebook
- Tablet computers such as iPads
- Mobile/cellular phones
- Smartphones
- Any mobile device capable of storing data and connecting to an unmanaged network.

The goal of this policy is to protect the integrity and confidential data that resides within Harrison College's technology infrastructure. This policy intends to prevent this data from being deliberately or inadvertently stored insecurely on a mobile device or carried over an insecure network where it can potentially be compromised. A breach of this type could result in loss of information, damage to critical applications, financial loss, and damage to the college's public image. Therefore, all users employing a mobile device connected to an unmanaged network outside of Harrison College's direct control to backup, store, and otherwise access data of any type must adhere to Harrison College's defined processes for doing so. As part of our safeguarding and statutory compliance adherence this policy articulates our intentions to have appropriate and effective filtering and monitoring systems in place on school devices, networks and personal use devices.

Furthermore, this policy relates to UK Data Protection 2018 legislation including UK GDPR which places duties on organisations and individuals to process personal information fairly and lawfully and to keep the information they hold safe and secure.

**Responsibility**

Governing bodies, proprietors and senior leaders of the college have a strategic leadership responsibility for their college's safeguarding arrangements and must ensure that they comply with their duties under legislation. In accordance with KCSIE 2023 the designated safeguarding lead should take lead responsibility for safeguarding and child protection, including online safety and understanding the filtering and monitoring systems and processes in place at Harrison College.

The Principal should ensure that the policies and procedures, are understood, and followed by all staff and those associated with the provision. Therefore, this policy is shared with staff, students, parents, carers and other specific users of Harrison College's IT provision so we can support, advise and help everyone to feel confident on welfare, safeguarding and child protection matters.

**Applicability**

This policy applies to all Harrison College employees and students, including full and part-time staff, faculty and other consultants who utilise either College-owned or personally-owned mobile device to access, store, back up, relocate or access any resources / information. Such access to the resources / information is a privilege, not a right. Consequently, employment at Harrison College does not automatically guarantee the initial and ongoing ability to use these devices to gain access to networks and information.

The policy addresses a range of threats:

- Loss - Devices used to transfer, or transport work files could be lost or stolen
- Theft - Sensitive District data is deliberately stolen and sold by an employee
- Copyright - Software copied onto a mobile device could violate licensing

- Malware Viruses, Trojans, Worms, Spyware and other threats could be introduced via a mobile device
- Compliance - Loss or theft of financial and/or personal and confidential information / data could expose the college to the risk of non-compliance with various identity theft and privacy laws
- Behaviour and safety – misuse of IT and mobile phones which can cause harm, distractions and criminal activity on-line and through social media.

Addition of new hardware, software, and/or related components to provide additional mobile device connectivity will be managed at the sole discretion of IT (for reference, IT refers to the Principal with the support of a third party agent). Unauthorised use of mobile devices to back up, store, and otherwise access any college related information/data is strictly forbidden.

This policy is complementary to any previously implemented policies dealing specifically with data access, data storage, data movement, and connectivity of mobile devices to any element of the College network.

**Policy and Appropriate Use**

It is the responsibility of any employee or student at the College, who uses a mobile device to access resources, to ensure that all security protocols normally used in the management of data on conventional storage infrastructure are also applied here. It is imperative that any mobile device that is used to conduct College business be utilised appropriately, responsibly, and ethically. Failure to do so will result in immediate suspension of that user's account.

Electronic devices, including mobile phones, can contain files or data which relate to an offence, or which may cause harm to another person. This includes, but is not limited to, indecent images of children, pornography, abusive messages, images or videos, or evidence relating to suspected criminal behaviour. Based on this, the following rules must be observed:

**Access Control**

1. IT reserves the right to refuse, by physical and non-physical means, the ability to connect mobile devices. IT will engage in such action if it feels such equipment is being used in such a way that puts the College's systems, data, student, staff and faculty at risk.
2. Prior to initial use on the network or related infrastructure, all mobile devices must be registered with IT. IT support will maintain a list of approved mobile devices and related software applications and utilities as needed.
3. End users who wish to connect such devices to non-College network infrastructure to gain access to College data must employ, for their devices and related infrastructure, security measures deemed necessary by the IT department such as updated software, anti-virus software, and personal firewall. All mobile devices attempting to connect to the network through an unmanaged network (i.e. the Internet) will be inspected using technology centrally managed by the IT department. Devices that have not been previously approved by IT, are not in compliance with IT's security policies, or represent any threat to the District network or data will not be allowed to connect. Laptop computers or personal PCs may only access the network using a Virtual Private Network (VPN) connection.
4. Employees using mobile devices and related software for network and data access will, without exception, use secure data management procedures. All mobile devices must be protected by a strong password.
5. All users of mobile devices must employ reasonable physical security measures. End users are expected to secure all such devices used for this activity whether or not they are actually in use and/or being carried. This includes, but is not limited to, passwords, encryption, and physical control of such devices whenever they contain TREC data.
6. IT will manage security policies, network, application, and data access centrally using whatever technology solutions it deems suitable. Any attempt to contravene or bypass said security

implementation will be deemed an intrusion attempt and will be dealt with in accordance with the College's overarching security policy.

7. Employees, contractors, full time faculty, part time faculty and temporary staff will follow all College sanctioned data removal procedures to permanently erase College specific data from such devices once their use is no longer required, or on termination of their contract with Harrison College.
8. In the event of a lost or stolen mobile device it is incumbent on the user to report this to IT immediately. The device will be remotely wiped of all data and locked to prevent access by anyone other than IT. If the device is recovered, it can be submitted to IT for reprovisioning.
9. Employees, contractors, full time faculty, part time faculty and temporary staff will make no modifications of any kind to College-owned and installed hardware or software without the approval of the Principal. This includes, but is not limited to, any reconfiguration of the mobile device.

**Organisational Protocol**

The Principal, IT department or DSL can and will establish audit trails and these will be accessed and used without notice. Such trails will be able to track the attachment of an external device to a PC, and the resulting reports may be used for investigation of possible breaches and, or misuse. The end user agrees to and accepts that their access and or connection to the College's networks may be monitored to record dates, times, duration of access, etc., in order to identify unusual usage patterns or other suspicious activity that may fall under our safeguarding and on-line filtering and monitoring duties. This is done in order to identify accounts and computers that may have been compromised by external parties. In all cases, data protection remains the college's highest priority. Harrison College can decide where these records are kept, but they must be kept confidential, held securely and comply with the Data Protection Act 2018 and the UK General Data Protection Regulation (UK GDPR)

Harrison College may wish to consider using CCTV footage to decide whether to further investigate a possible breach or to conduct a search for an item.

**Email**

There may be occasions where staff work outside of college hours due to personal commitments. Leadership at Harrison College do not discourage this as we understand that staff manage their own workload for their own circumstances. However, any work-related emails must be sent by 6pm or must have a delay delivery until 7.30am the next working day. This is to protect all employee's home, life balance.

**Policy Non-Compliance**

Failure to comply with this policy may, at the full discretion of the College, result in the suspension of any or all technology use and connectivity privileges, disciplinary action, and possibly termination of employment.

Confiscation and search:

For students and staff, the confiscation of their mobile phone or device may be deemed necessary. If they do not voluntarily hand over their phone, in an attempt to ensure the safety and welfare of our students and employees the college may be required to search an individual to locate and confiscate the device or phone posing a threat to the welfare and safety of others. Before conducting a search of an individual, it is vital that we consider their obligations under the European Convention on Human Rights. Under Article 8, students and employees have a right to respect for their private life and a right to expect a reasonable level of personal privacy.

The powers to search in the Education Act 1996 are compatible with Article 8. When exercising those powers lawfully only the principal or a nominated person by the Principal such as the DSL or senior member of staff can carry out a search and they should have no difficulty in demonstrating that they have acted in accordance with Article 8.

Before any search is carried out the Principal, DSL/DDSL or nominated person will ensure that a culture of safe, proportionate and appropriate searching is maintained, which safeguards the welfare of all students and staff.

An appropriate location for the search should be found. Where possible, this should be away from other students. The search must only take place on the college premises or where the member of staff has lawful control or charge of the student, for example on a school trip, residential or travelling on the minibus.
The law states the member of staff conducting the search must be of the same sex as the individual being searched. There must be another member of staff present as a witness to the search. We may search a outer clothing, pockets, bags, possessions, desks or lockers.

Any search by a member of staff and all searches conducted by police officers should be recorded in the college's CPOMs safeguarding reporting system, including whether or not an item is found. Harrison college should consider that in some circumstances it might also be necessary to inform parents or carers of a search for a mobile phone, device or other item banned by the college policy.

**Online Safety**

Harrison College are aware of the unique risks associated with online safety and recognise the additional risks that students with special educational needs and disabilities (SEND) face online, for example, from bullying, grooming and radicalisation. We therefore need to be confident that our policies and processes have the capability to support children with SEND to stay safe online at college.

For this reason, and those associated with distraction and maintaining an environment where students can engage with the learning free from worry and harassment, Harrison College will exercise its right to limit or ban the use of mobile phones and BYOD when it sees fit. For students, mobile phones should not be used in college learning time and should be kept in lockers or handed in to a member of staff for safe keeping. Students will normally be allowed to access their phones during social times, lunch and breakfast club. For staff and other adult users, mobile phones should not be used within college learning time unless prior consent has been agreed with the DSL or Principal. Phones should be kept in the locker or switched off or silent on their person.

Any member of staff or a student of Harrison College who receives abuse online should report directly to the Principal or Designated Safeguarding Lead.
If a member of staff finds a pornographic image, they may dispose of the image unless they have reasonable grounds to suspect that its possession constitutes a specified offence (i.e. it is extreme or an indecent image of a child) in which case it must be delivered and reported to the police as soon as is reasonably practicable. Members of staff should never intentionally view any indecent image of a child (also sometimes known as nude or semi-nude images). Staff must never copy, print, share, store or save such images. When an incident might involve an indecent image of a child and/or video, the member of staff should confiscate the device, avoid looking at the device and refer the incident to the designated safeguarding lead (or deputy) as the most appropriate person to advise on the colleges response.

Members of staff should use their judgement to decide to return, retain or dispose of any other items banned under the school rules.

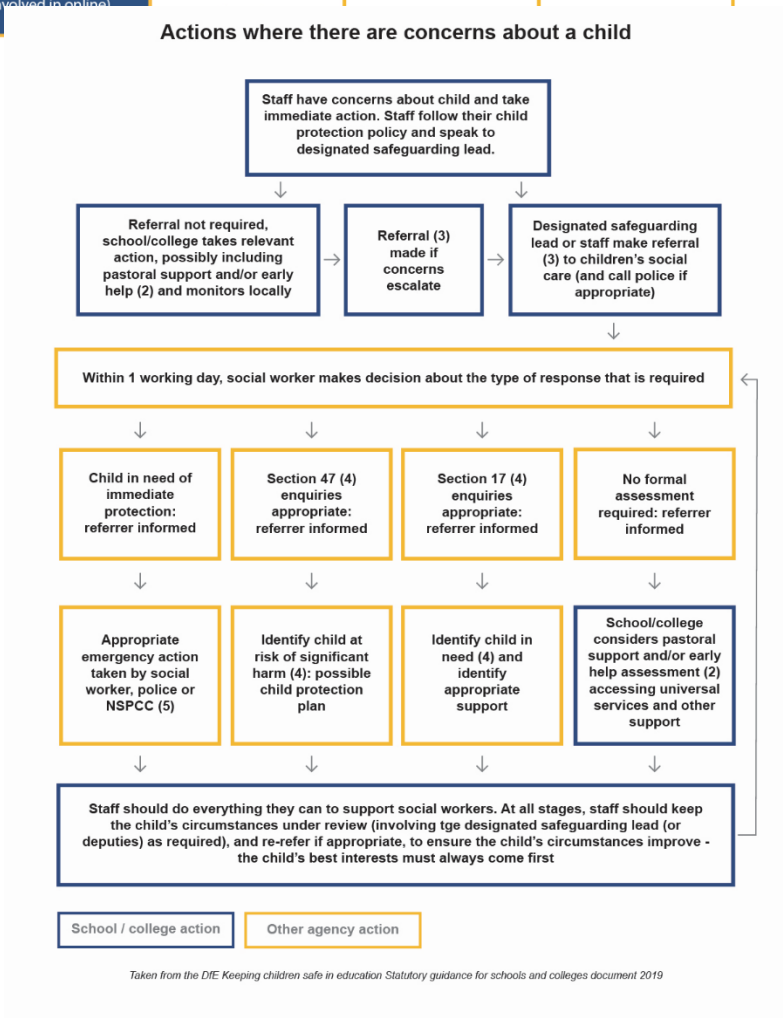
This policy should be read in conjunction with our Online safety policy contained within our Safeguarding and child protection policies.

**Making a Referral**

- A referral will be made to the Local Authority social care team
- Any cases referring to radicalisation will be referred to Channel
- Any cases where a crime may have been committed will be referred to the Police

## Making a referral: The Three C's

| | Commercial | Aggressive | Sexual | Values |
|---|---|---|---|---|
| **Content** (Types of content children might see) | • Adverts<br>• Spam<br>• Sponsorship | • Violence / hate | • Pornographic and unwelcomed sexual content | • Bias, racist, misleading information or advice |
| **Contact** (Types of interaction which children may have online) | • Tracking<br>• Harvesting personal information | • Bullying<br>• Harassment<br>• Stalking | • Meeting strangers<br>• Grooming | • Self-harm and unwelcomed persuasions |
| **Conduct** (Types of behaviour a child might get involved in online) | • Illegal downloading<br>• Hacking<br>• Gambling<br>• Financial scams | • Bullying<br>• Harassment | • Creating or uploading inappropriate material | • Misleading information or advice |



**Remote learning**
This section of the AUP relates, specifically, to remote learning and is in place to safeguard all members of Harrison College community when taking part in remote learning following any full or partial closures. As part of KCSIE 2023, Working Together to Safeguard Children 2018 and the DfE's published filtering and monitoring standards, the college ensures that we have appropriate filtering and monitoring processes in place to be able to keep our students safe when embarking on online and remote learning.

Staff will be trained and updated on the safe use of remote learning and where possible achieve the National Online Safety qualifications and webinars.

**Leadership Oversight and Approval**

1. Remote learning will only take place using Microsoft Teams and SharePoint
    - Teams has been risk assessed and approved by the Principal, DSL and Senior Leadership Team (SLT).
2. Staff will only use Harrison College managed or specific, approved professional accounts with learners, parents and carers.
    - Use of any personal accounts to communicate with learners, parents or carers is not permitted unless previously agreed by the DSL or Principal.
        - Any pre-existing relationships or situations which mean this cannot be complied with will be discussed with the Designated Safeguarding Lead (DSL).
    - Staff will use work-provided and approved equipment where possible e.g. a College laptop, tablet, or other mobile device. Where a member of staff is using their own device, there are clear expectations in relation to safeguarding and data security, e.g. using strong passwords, suitable levels of encryption, logging off or locking devices when not in use etc.
3. Online contact with learners, parents and carers will not take place outside of College operating times as defined by SLT, unless previously agreed by the DSL or Principal.
4. All remote lessons will be formally timetabled; a member of SLT, DSL is able to 'drop in' and monitor this at any time.
5. Live streamed remote learning sessions will only be held with approval and agreement from the Principal or DSL.

**Data Protection and Security**

6. Any personal data used by staff and captured by Teams when delivering remote learning will be processed and stored with appropriate consent and in accordance with our data protection policy.
7. All remote learning and any other online communication will take place in line with current College confidentiality expectations as outlined in our Safeguarding policy.
8. All participants will be made aware that Teams records activity.
9. Staff will not record lessons or meetings using personal equipment unless agreed and risk assessed by SLT and in line with our data protection policy requirements.
10. Only members of Harrison College community will be given access to Teams/SharePoint.
11. Access to Teams/SharePoint will be managed in line with current IT security expectations as outlined in the ICT Acceptable Usage policy.

**Session Management**

12. Staff will record the length, time, date, and attendance of any sessions held.
13. Appropriate privacy and safety settings will be used to manage access and interactions. This includes:
    - Language filters, disabling/limiting chat, staff not permitting learners to share screens, keeping meeting IDs private, use of waiting rooms/lobbies or equivalent.
14. When live streaming with learners:
    - contact will be made via learners' College provided email accounts and logins.
    - staff will mute/disable learners' videos and microphones.
15. Live 1 to 1 sessions will only take place with prior approval from the Principal/COO/ DSL.
16. A pre-agreed invitation/email detailing the session expectations will be sent to those invited to attend.
    - Access links should not be made public or shared by participants.
    - Learners and/or parents/carers should not forward or share access links.
17. Alternative approaches and or access will be provided to those who do not have access, e.g. the loan of a College device.

**Behaviour Expectations**

18. Staff will model safe practice and moderate behaviour online during remote sessions as they would in the classroom.
19. All participants are expected to behave in line with existing College policies and expectations. This includes:
    - Appropriate language will be used by all attendees.
    - Staff will not take or record images for their own personal use.
20. Staff will remind attendees of behaviour expectations and reporting mechanisms at the start of the session.
21. When sharing videos and/or live streaming, participants are required to:
    - wear appropriate dress.
    - ensure backgrounds of videos are neutral (blurred if possible).
    - ensure that personal information and/or unsuitable personal items are not visible, either on screen or in video backgrounds.
22. Educational resources will be used or shared in line with our existing teaching and learning policies, taking licensing and copyright into account.

**Policy Breaches and Reporting Concerns**

23. Participants are encouraged to report concerns during remote and/or live streamed sessions:
24. If inappropriate language or behaviour takes place, participants involved will be removed by staff, the session may be terminated, and concerns will be reported to the Principal or DSL.
25. Inappropriate online behaviour will be responded to in line with existing policies such as acceptable use of technology, allegations against staff, anti-bullying and behaviour.
26. Sanctions for deliberate misuse may include restricting or removing use, confiscating devices and contacting police if a criminal offence has been committed.
27. Any safeguarding concerns will be reported to the Designated Safeguarding Lead, in line with our child protection and safeguarding policy.

**Declaration**

I understand that the College's IT acceptable use policy (including the sections relating to remote learning) applies to the use of the College's ICT systems or hardware inside or outside College. Failure to comply with this policy may result in disciplinary action.

I have read and understood the above and agree to use the College's ICT system, my own devices in and outside of College and when making communications related to College business, within the guidelines of this document.

Staff / student / user name:…….

Signature: …… Date: ……