ASHLEY COLLEGE

Digital Safety/Social Media and Acceptable Use of Property Policy

(Adopted from LA Policy of April 2020)

Date approved:	Autumn 2026
Next review:	Autumn 2027
Legal updates may precipitate changes	
Version:	Final
Status:	Active

Contents

1. Introduction 3

2. Purpose 3

3. Roles and responsibilities 4

4. Definitions 4

5. Personal use of social media 5

6. School-sanctioned use of social media 6

7. Mobile technologies 6

8. School Sanctioned remote learning platforms 6

9. Communications 7

10. Support for staff 7

11. Acceptable use of school digital property 8

12. Monitoring of this policy 9

13. The law 9

14.Wearable……10,11…

Appendix 1. How to stay 'Cybersafe' 11

Appendix 2. Service Provider Contacts 13

Appendix 3. Digital Safety Lead 14

Appendix 4: Acceptable Use Policy Statements 15

Appendix 5 'Metaverse' and Virtual Reality guidance 18

Appendix 6. Staff Declaration 22

1. Introduction

Computing and the use of digital devices is seen as an essential resource to support teachers and actual learning; as well as playing an important role in the everyday lives of children, young people and adults. The widespread availability and use of digital devices and social media applications brings opportunities to understand, engage, and communicate in new and exciting ways. It is important that we are able to use these technologies and services effectively and flexibly. However, it is also important to ensure that we balance this with our duties to our school, the community, our legal responsibilities and our reputation. For example, our use of social networking applications has implications for our duty to safeguard children and young people.

Computing and Information and Communication Technology (ICT) covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of computing within our society as a whole.

This policy applies to the school management committee, all teaching/support and other staff, whether employed directly by the school **or through a hiring organisation (e.g. agency),** external contractors providing services on behalf of the school, teacher trainees and other trainees, volunteers and other individuals who work for or provide services on behalf of the school. These individuals are collectively referred to in this policy as Staff.

This policy provides a good practice approach to using the Internet and social media and will ensure that the use of social media is effective, lawful and does not compromise the school's reputation, school information or computer systems/networks.

Examples of unacceptable ICT practice include:

- forwarding of school confidential messages to external locations
- distributing, disseminating or storing images, text or materials that might be considered indecent, pornographic, obscene or illegal
- distributing, disseminating or storing images, text or materials that might be considered discriminatory, offensive or abusive, in that the context is a personal attack, sexist or racist, or might be considered as harassment
- accessing copyrighted information in a way that violates the copyright
- breaking into the school's or another organisation's system or unauthorised use of a password/mailbox
- broadcasting unsolicited personal views on social, political, religious or other non-school related matters
- transmitting unsolicited commercial or advertising material
- undertaking deliberate activities that waste staff effort or networked resources
- introducing any form of computer virus or malware into the school network
- use of school communications systems to set up personal businesses or send chain letters

2. Purpose

The purpose of the policy is to:

- ensure staff use digital devices and social media responsibly, to avoid bringing the School into disrepute.
- safeguard all children and staff.

- ensure that where information is provided through social media regarding the School, this is l representative of the school.

3. Roles and responsibilities

The management committee will ensure that this policy will reviewed and monitored as appropriate.

The Headteacher will ensure that the School has a nominated Digital Safety Lead (DSL) tasked with overseeing and managing the recording, investigation and resolution of digital safety incidents. Contact details for the School's DSL is attached as an appendix to this policy. The nominated DSL will be suitably trained in order to undertake this role. The Headteacher and Senior Leadership Team will familiarise themselves with government guidance on digital safety and in particular the prevention of bullying (see website: https://www.gov.uk/government/publications/preventing-and-tackling-bullying).

All staff will familiarise themselves with this policy and will be provided with relevant information, guidance and training in digital safety insofar as is appropriate to the discharge of their duties. All staff and management committee are expected to read and sign the declaration attached at Appendix 4 to confirm they have read and understood the Digital Safety/Social Media and Acceptable Use Policy.

4. Definitions

Social media is a collection of on-line communication channels that allow people to create, share or exchange information, conversations, pictures and videos.

Social networking applications can include but are not limited to Facebook and Twitter, Instagram, Snapchat, messaging on MSN and on mobile phones, blogs, LinkedIn, online discussion forums, YouTube, 'Micro blogging' applications, online gaming environments, and comment streams on public websites such as newspaper site etc. The growth of social media has been boosted by the fact that there is no longer a need to access it through a personal computer. Digital devices such as smartphones, tablets, laptops etc. easily connect users to the internet.

Cyber bullying is defined as any use of social media or communication technology to bully an individual or group e.g. taunts on line, by texts using social media platforms.

Many of the principles of this policy also apply to other types of online presence such as virtual worlds. The absence of, or lack of, explicit reference to a specific website or service does not limit the extent of the application of these guidelines. The internet and social media is driven by fast paced evolving technology. Accordingly, it is not possible for the policy to cover every eventuality, but the principles set out in this policy must be followed irrespective of the medium.

Within this policy there is a distinction between the uses of school-sanctioned social media and personal use of social media.

5. Personal use of social media

- Staff employed by the School are entitled to use whatever system they like outside their working time and working persona, to engage in the social aspects of the media. However, great care should be taken to ensure the private/work line is not crossed. It is good practice not to mention work, your opinions of your colleagues or processes and projects on your own private social media networks. There is also a recognition that staff/school leaders may use their social media accounts for professional use to share best practice; however where this occurs confidentiality issues must be strictly observed. Where the school's behaviour policy/code of conduct explicitly prevents mentioning work/opinions of colleagues/processes/projects within private or public social media networks, this should be observed.
- Staff need to be aware of their online reputation and have to recognise that comments that they make online can be seen by others, particularly when using social networking sites. Staff should regard private social media with privacy settings as potentially public (i.e. viewed and shared to third parties) and anything they publish, whether they identify themselves as school employees or not, may bring the School into disrepute or call into question their suitability to work at the school, which could result in dismissal. Employees should ensure they monitor the responses of comments made on their own social media accounts and remove them if damaging to the school or its employees where this is brought to their attention.
- There is an acknowledgment that school staff may/will have pre-existing engaged communications with parents from the school community. However, school staff are advised not to invite, accept or engage in communications with new parents and should not accept or engage in communications with children from the school community in any personal social media whilst in employment at the School**.** Those pre-existing communications should be responsible and comply with the points listed below.
- Any communication received from children on any personal social media site must be reported to the DSL who will be responsible for referring this onto the designated safeguarding lead.
- If any member of staff is aware of any inappropriate communications involving any child in any social media, these must immediately be reported as above.
- School staff are strongly advised to set all privacy settings to the highest possible levels on all personal social media accounts.
- All email communication between staff and members of the school community on school business must be made from an official school email account.
- Staff should not use personal email accounts or mobile phones to make contact with members of the school community on school business, nor should any such contact be accepted, except in circumstances given prior approval by the Headteacher.
- Staff are not permitted to refer to specific individual matters related to the School and members of its community on any social media accounts.
- Staff are also advised to consider any reputation issues to the School in any posts or comments related to the School on any social media platforms.
- Special consideration may be given on the above three points if it is for the purpose of trade union activity; which should be conducted within private member-only groups and in line with the union's own GDPR policies, and should not be shared or copied outside these private memberships. Staff are still expected to observe the school's/trade union's codes of conduct in such communications and where appropriate utilise the school's procedures to address any concerns they may have with the school or its staff.
- Staff should not accept any current pupil of any age or any ex-pupil of the School under the age of 18 as a friend, follower, subscriber or similar on any personal social media account.

- Where it is found that staff engage in the unacceptable use of social media in their private time using their personal social media accounts, it can be treated as misconduct (including gross misconduct) under the School's policies.

6. School-sanctioned use of social media

When using social media for educational/promotional purposes, the following practices should be observed.

- The content of any school-sanctioned social media site should be solely professional and should reflect well on the school. Staff should use their work account, rather than their private social media account, to respond to school comments/mentions on a school sanctioned social media platform e.g. Twitter, Facebook etc.
- Staff must not publish photographs of children without the written consent of parents/ carers, identify by name any children featured in photographs, or allow person-identifying information to be published on school social media accounts
- Care must be taken that any links to external sites from the account are appropriate and safe
- Any inappropriate comments on, or abuse of, school-sanctioned social media should immediately be reported to a member of the Senior Leadership Team (SLT) or the nominated digital safety lead. Where possible, care should be taken to preserve evidence of inappropriate comments/abuse (e.g. text, email, voicemail, website, instant message etc.) by taking screen prints of messages, web pages, images etc. in order that it can be investigated and relevant action taken.
- The DSL in conjunction with the Headteacher will be responsible for determining the School's responses to school sanctioned social media platforms. This responsibility may be delegated to other staff from time to time.

7. Mobile technologies

- Students hand their mobile phones in to reception for safe storage on arrival and collect them on departure.
- The School allows staff to bring in personal mobile phones and devices for their own use during designated times outside of the classroom. These are normally not to be used whilst children are present.
- Staff should not use their own personal devices to contact pupils or parents either in or out of school time. Any exception to this must be authorised by school leaders and appropriate measures put in place.
- Staff are not permitted to take photos or videos of pupils. If photos or videos are being taken as part of the school curriculum or for professional purposes, the school equipment will be used for this. Only school phones should be used on school trips for the purposes of recording pictures/videos etc.
- The School is not responsible for the loss, damage or theft of any personal mobile device.

8. School Sanctioned remote learning platforms

- Staff will only use school sanctioned platforms which have been assessed and approved by the Senior Leadership Team for remote learning in the school.
- The school has adopted the Template Acceptable Use Policy (AUP) for Remote Learning and Online Communication (see appendix 4).

9. Communications

When using communication technologies, staff should consider the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Staff should be aware that email communications are monitored. Staff should use the school email services to communicate school business. The exception is that personal emails and trade union email accounts can be used in addition for trade union communications as long as it is used in line with the unions' own GDPR policies and the school's/union's codes of conduct.
- Email use is encouraged where this supports the goals and objectives of the school. However, staff using email must ensure that they comply with current legislation, use email as a professional communication, do not create unnecessary risk to the school, children or staff by misuse, be aware that email may be forwarded without their knowledge and ensure that communications going outside of the school represent the school
- The use of email is a valuable communication tool. Nevertheless, misuse(s) of this facility can potentially have a negative impact upon staff morale, corrupt the school system or damage the reputation of the school/individual. Special care should be taken to avoid such misuse. The school's email resources are provided for school related communication purposes. E-mails should not, as a matter of course, be regarded as private and any e-mail sent through the School domain remains the property of the School. The Laws regarding the use of electronic mail are fairly stringent. Certain offenses regarding libel and publication of obscene material also apply to items transmitted through e-mail. Therefore, in order to protect pupils and staff the school maintains the right to examine any systems and inspect any data recorded in those systems including school email accounts.
- Staff must immediately report to their line manager, Digital Safety Lead or Headteacher, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature.
- Any digital communication between staff and the school community must be professional in tone and content. These communications may only take place on official (monitored) school systems.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.
- Photos of staff should not be posted on the school website unless staff have given consent for this. Schools may wish to use their established GDPR consent mechanisms to ensure the school complies with this requirement. Schools should ensure periodic review of such mechanisms to ensure they are robust in this regard.

Staff should also refer to the list of Cybersafe –Do's and Don'ts in Appendix 1 of this policy.

10. Support for staff

Where staff have been the target of inappropriate, offensive, threatening, bullying/cyberbullying communication through digital means (whether in their professional or private life) which impacts their ability to carry out their role effectively, they should expect the School to:

- record such incidents in writing
- investigate such incidents on behalf of staff.
- respond to such incidents in a timely and appropriate manner, or support the member of staff concerned to do so.

- provide appropriate support, or information enabling them to access appropriate personal support e.g. employee assistance scheme or occupational health.
- support the member of staff to contact the police, external agencies or service provider where appropriate (see Appendix 2 for contact details for service providers).
- Take appropriate action against the perpetrator in line with the relevant school policies where this falls within the schools jurisdiction.

11. Acceptable use of school digital property

- Staff are responsible for any digital property belonging to the organisation that is under their control or in their possession and must take proper care of any such items.
- Staff must take good care of school digital property, both when it is used in the workplace and when it is used outside the organisation's premises (e.g. at home).
- Staff must not make modifications to the school's digital property (for example, upgrades to a laptop) without the prior approval in writing of the School.
- Staff must not use school digital property to carry out any illegal activities or activities that might bring the organisation into disrepute (for example, using a laptop to visit inappropriate websites).
- By act or omission, staff must not allow school digital property to be lost or damaged (for example, by not securing property properly or leaving it in a public place such as on public transport). However, the school should ensure they are insured, where possible, for such eventualities if staff are required to participate in remote working and/or working from home.
- Staff must not remove any school digital property from the school's premises without the prior approval of the Headteacher or Chair of Governors.
- On termination of their employment, staff will be required to return the school's digital property on the date specified by the Headteacher, which will normally be their last day at work. It is the member of staff's responsibility to return school digital property.
- The School reserves the right to withhold the whole or any part of a member of staff's wages up to the market value of the school's digital property if he/she does not return that property by the set date. The amount withheld will be based on the estimated value of the property at that time.
- In appropriate cases, the school may contact the police about the unreturned property and/or issue civil proceedings against the member of staff for breach of contract and/or trespass to goods to the extent that any outstanding wages withheld do not cover the current market value of the property not returned.

Filtering and Monitoring

Filtering refers to the technology preventing access to harmful or inappropriate content, whilst monitoring refers to the practical steps staff take to ensure harmful or inappropriate access is not made.

Through our association with London Grid for Learning and Imperio we make sure that the school's filtering and monitoring systems are functional and effective. All school devices used on or off site are subject to filtering and monitoring procedures.

Staff undertake training to understand the risks of poor filtering and monitoring, and know how to share their concerns.

Also refer to Safeguarding and Child Protection Policy and DfE Filtering and Monitoring Standards for Schools and Colleges.

12. Monitoring of this policy

Any violation of this policy may be considered as potentially gross misconduct under the school's

- Disciplinary Policy and Procedure (staff)
- Code of Conduct (staff)
- Safeguarding Policy
- Code of Practice (management committee)

which may result in disciplinary action being taken up to and including dismissal.

All staff and Management Committee are encouraged to report any suspicions of misuse to the Headteacher/Digital Safety Lead. If the Headteacher receives a disclosure that staff or a member of management committee is using digital devices/social networking in an inappropriate way, as detailed above, this should be dealt with in accordance with the Safeguarding Policy and/or Disciplinary Policy and Procedure

The school has a duty of care to investigate and work with children and families where there are reports of cyber bullying/misuse of social media during out of school hours.

13. The law

All members of staff should bear in mind that information they share through social networking applications, even if they are on private spaces, might be still subject to copyright, The General Data Protection Regulation, The Data Protection Act 2018 and Freedom of Information legislation, the Safeguarding Vulnerable Groups Act 2006 and other legislation. They must also operate in line with government guidance on safeguarding children and the school's Equalities and Child Protection policies.

Whilst there is no one specific offence of cyber bullying, certain activities can be criminal offences under a range of different laws, including:

- The Protection from Harassment act 1997
- The Malicious Communications act 1988
- S.127 of the Communication act 2003
- Public Order Act 1986
- The Defamation Acts of 1952, 1996 and 2013

A school cannot be 'defamed'; only individuals or groups of individuals can bring action for defamation. Staff who are concerned that comments posted about them are defamatory in nature, should seek advice from their line manager/Headteacher.

The Headteacher may seek HR/legal advice on any matters related to the potential misuse of social media.

Wearable Technology

The School recognises that wearable technology devices (such as smartwatches, fitness trackers, smart glasses, and similar devices) are increasingly common and may have connectivity and recording capabilities. To ensure the safety and privacy of all members of the school community, the following guidelines apply:

Student Use:

- Students are not permitted to wear devices with connectivity, recording, or communication capabilities during the school day, including smartwatches that can make calls, send messages, take photos, or access the internet, and smart glasses with recording functions
- Any such devices brought to school must be handed in to reception for safe storage on arrival and collected on departure, in line with the school's mobile phone policy
- Basic fitness trackers without communication or recording functions may be permitted at the discretion of the Headteacher

- **Exceptions for accessibility and medical needs:**
    - Wearable devices required for medical monitoring (such as continuous glucose monitors or medical alert devices) are permitted with prior agreement from the Headteacher
    - Smart glasses or other assistive wearable technology required to support visual impairment or other disabilities are permitted where they form part of a student's reasonable adjustments or Education, Health and Care Plan (EHCP)
    - Parents/carers must inform the school in writing of any such devices, their purpose, and their capabilities
    - The school will work with families to ensure such devices are configured appropriately to balance accessibility needs with safeguarding requirements (for example, by disabling unnecessary recording or communication features where possible)
    -

Staff Use:

- Staff may wear personal wearable devices during the school day, but must ensure these devices:
    - Do not compromise pupil safety or privacy
    - Are not used to record images, video, or audio of pupils without proper authorisation and parental consent
    - Do not distract from their professional duties
    - Comply with all other aspects of this policy regarding personal devices and social media

- **Staff with accessibility needs:**
    - Staff who require wearable technology for accessibility purposes (such as smart glasses for visual impairment or hearing aids with connectivity features) should discuss their needs with the Headteacher to ensure appropriate adjustments are made
    - Such devices will be permitted where they are necessary reasonable adjustments under the Equality Act 2010
    - Staff must ensure that any recording or communication features not essential to the accessibility function are disabled during working hours
- Any use of wearable technology for educational or school-sanctioned purposes must be approved in advance by the Senior Leadership Team
- Staff should be mindful that wearable devices with 'always-on' voice assistants or automatic recording features must be disabled or removed when working with pupils

Visitor Use:

- All visitors to the school, including parents/carers, contractors, volunteers, and external professionals, must be informed that the use of wearable technology with recording capabilities (including smart glasses and smartwatches with cameras) is not permitted on school premises without prior authorisation from the Headteacher
- This requirement will be clearly communicated through:
    - Signage at the school entrance
    - The visitor sign-in process at reception
    - Information provided to contractors and regular visitors in advance

- **Exceptions for visitors:**
    - Visitors who require wearable technology for accessibility or medical purposes should inform reception staff upon arrival
    - The school will make reasonable adjustments to accommodate such needs whilst maintaining safeguarding standards
    - Where recording capabilities cannot be disabled, the visitor may be asked to be accompanied at all times or restricted to certain areas of the school
- Visitors found to be using wearable technology inappropriately or without authorisation may be asked to leave the premises immediately and may be prohibited from future visits

The School reserves the right to review and update this guidance as wearable technology continues to evolve.

Appendix 1. How to stay 'Cybersafe'

How to Stay 'Cybersafe' – Do's and Don'ts for school staff

DO	DON'T
• be aware of your on-line reputation, which consists of information you post about yourself and information posted by others, and consider that when seeking employment, many prospective employers will use publicly available on-line information. Type your name into various search engines to see what information there is about you on the internet. Remember, the internet never forgets! • keep passwords secret and protect access to accounts – always log off from any device that you have been using, even if you are only stepping out of the room for a moment and ensure that all phones and tablet devices are secured with a passcode;	• post information and photos about yourself, or school-related matters, publicly that you wouldn't want employers, colleagues, pupils or parents to see; • befriend pupils or other members of the school community on social networking sites. (You should consider carefully the implications of befriending parents or ex-pupils). • personally retaliate to any incident, bullying messages; • criticise your school, pupils or pupils' parents online.

• regularly review your privacy settings on social media sites and your devices (mobile phone, tablet, laptop etc.); • discuss expectations with friends – are you happy to be tagged in photos? • be aware that, increasingly, individuals are being held to account in the courts for the things they say on social networking sites; • keep personal phone numbers private and don't use your own mobile phones to contact pupils or parents; • use a school mobile phone when on a school trip; • keep a record of your phone's unique International Mobile Equipment Identity (IMEI) number, keep phones secure while on school premises and report thefts to the police and mobile operator as soon as possible (Note: you can find out your IMEI number by typing *#06# on your handset – the number will be displayed on the screen); • ensure that school rules regarding the use of technologies are consistently enforced; • report any incident to the appropriate member of staff in a timely manner; • keep any evidence of an incident, for example by not deleting text messages or e-mails and by taking a screen capture of material (staff need to be aware that taking a screenshot of content which is potentially illegal could result in staff committing a criminal offence) including the URL or web address. • use school e-mail address only for work purposes. • be aware that if you access any personal web-based e-mail accounts via the school network, that these may be subject to the school's internet protocol which could include monitoring and surveillance. • request assurances from management that any e-mails marked 'personal' and/or 'union business' will not be read without your prior consent.	

• raise genuine concerns about your school or certain members of staff using your employer's whistle blowing or grievance procedure.	

More helpful tips are available from the UK Safer Internet Centre at www.saferinternet.org.uk under 'Advice and Resources'.

Appendix 2. Service Provider Contacts

Contact details for service providers

Service provider	From your mobile	Pay as you go	Pay monthly contracts
O2	202 (pay monthly) 4445 (pay as you go)	03448 090 222	03448 090 020
Vodaphone:	191	08700 776 655	08700 700 191
3	333	08707 330 333	08707 330 333
EE (Orange and T Mobile)	150	07953 966 250	07953 966 250
Virgin	789	0345 6000 789	0345 6000 789
BT		08000 328 751	08000 328 751

Appendix 3. Digital Safety Lead

Contact details for the School's Digital Safety Lead

Name	**Ranjna Shiyani**
School address	**Ashley College, Ashley Gardens, Wembley, Middx, HA9 8NP**
Contact number	**020 8937 3330**

Appendix 4: Acceptable Use Policy Statements

Ashley College Acceptable Use Policy Statements

Leadership Oversight and Approval

1. Remote learning will only take place using Google Classroom and Google Meets
    - G Suite has been assessed and approved Senior Leadership Team (SLT).
2. Staff will only use Ashley College managed accounts with learners and/or parents/carers.
    - Use of any personal accounts to communicate with learners and/or parents/carers is not permitted.
    - Any pre-existing relationships or situations which mean this cannot be complied with will be discussed with Louise Togher, Designated Safeguarding Lead (DSL).
    - Staff will use work provided equipment where possible e.g. a school laptop, tablet or other mobile device. If this is not possible staff must follow the guidance issued in the recently updated Working from Home Policy
3. Online contact with learners and/or parents/carers will not take place outside of the operating times as defined by SLT:
    - Normal school working times.
4. All remote lessons will be timetabled; a member of SLT and/or DSL is able to informally drop in at any time.
5. Live-streamed remote learning sessions will only be held with the approval and agreement of a member of SLT.

Data Protection and Security

6. Any personal data used by staff and captured by G Suite when delivering remote learning will be processed and stored with appropriate consent and in accordance with our data protection policy (link).
7. All remote learning and any other online communication will take place in line with current school confidentiality expectations as outlined in GDPR, Remote Learning, Working from Home, Safeguarding and Child Protection, Behaviour and Code of Conduct policies.
8. All participants must be made aware if recording is taking place. If staff are having a 1:1 session with a student it must be recorded as per guidance in Remote Learning policy.
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. All recordings must be saved to the google drive attached to your work account, as per remote working procedures.
10. All home tuition webcam lessons will be recorded and shared to Christine Cahillane who will ensure they are stored securely and deleted after 6 weeks. Once recordings have been downloaded and saved by above named staff, home tutors will be advised that they have to now delete from their G drive and provide photo evidence of such. These recordings will only be viewed should a safeguarding concern arise within the 6-week period they are stored prior to deletion.
11. Written consent for recording 1:1 home tuition webcam lessons will be collected from parents.
12. Only members of Ashley College community will be given access to G Suite
13. Access to G Suite will be managed in line with current IT security expectations as outlined in Remote Learning and Working from Home policies.

Session Management

Staff will record session details in their normal lesson logs.

14. Appropriate privacy and safety settings will be used to manage access and interactions. This includes:
    - disabling/limiting chat, Language filters, staff not permitting learners to share screens without permission, keeping meeting IDs private, not using waiting rooms/lobbies or equivalent.
15. When live streaming with learners:
    - contact will be made via **learners' Ashley College provided** email accounts and/or logins.
    - contact must be made with parent/carer at beginning and end of each session
    - staff will mute/disable learners' videos and microphones, if necessary.
    - If 2 members of staff are not present the session will be recorded for safeguarding purposes after consultation with SLT
16. Live 1 to 1 sessions will only take place with approval from a member of SLT.
17. A pre-agreed Google Classroom link detailing the session will be available 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.
    - If learners/parents/carers believe a link should be shared with others, they will discuss this with the member of staff running the session first.
    - Learners are encouraged to attend lessons in a shared/communal space or room with an open door 1:1 home tuition learners must be appropriately supervised by

a parent/carer or another appropriate adult who is acknowledged by the teacher at the start and end of each session.

18. Alternative approaches and/or access will be provided to those who do not have access ie
    - Where students do not have online access Ashley College or their mainstream school have provided the appropriate IT equipment.
    - All students have been provided with hardcopy work packs to cover WIFI unavailability

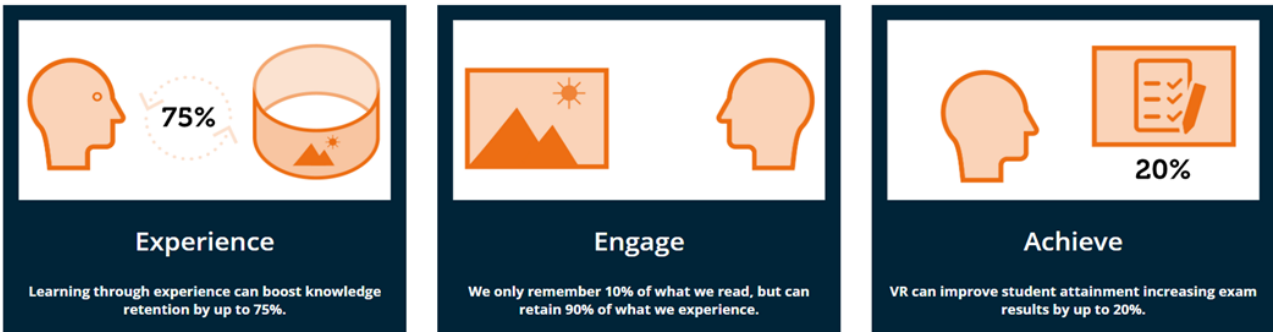
Behaviour Expectations

19. Staff will model safe practice and moderate behaviour online during remote sessions as they would in the classroom.
20. All participants are expected to behave in line with existing school 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.
    - Students will not record sessions
21. Staff will remind attendees of behaviour expectations and reporting mechanisms at the start of the session.
22. 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.
23. Educational resources will be used or shared in line with our existing teaching and learning policies, taking in account licensing and copyright laws.

Policy Breaches and Reporting Concerns

24. Participants are encouraged to report concerns during remote and/or live streamed sessions:
    For learners
    - Report concerns to the member of staff running the session
    - tell a parent/carer etc.
    - report to link tutor
    - if unable/unwilling to report during live session the schools email safeguarding@ashleycollege.brent.sch.ukk can be used or they can phone on 020 8937 3330 and report to Safeguarding Lead or Link Tutor

    For staff
    - report concerns to SLT or DSL
25. 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 SLT/ DSL
26. Inappropriate online behaviour will be responded to in line with existing policies such as acceptable use of technology, safeguarding and child protection, anti-bullying and behaviour. Sanctions for deliberate misuse may include
    - restricting/removing use
    - contacting police if a criminal offence has been committed
27. Any safeguarding concerns will be reported to Louise Togher, Designated Safeguarding Lead or either Ranjna Shiyani or Anne Marie Mika, Deputy Safeguarding Leads in line with our Safeguarding and Child Protection policy



Appendix 5 'Metaverse' and Virtual Reality guidance

The Metaverse

The metaverse is a shared virtual space where users can access content, play games, purchase items and build environments. The Metaverse in itself is a concept that is currently in development and certain aspects of the metaverse exist and use VR technology and benefits of VR headsets.

VR Headsets

At Ashley College, we believe there are clear educational benefits to be drawn from the use of virtual reality including: better engagement, increased stimulation, an innovative & enhanced learning experience and enhanced knowledge retention.

Evidence shows virtual reality has the capability to push the boundaries of teaching and helps students meet their learning goals. VR offers a great way to engage our students and enhance existing lessons.

At Ashley College, we place focus on how the technology can be used to aid a meaningful, rich learning experience not simply using technology for the sake of it: We believe learning should not be led by technology alone - teachers teach and technology can assist learning.

Virtual Reality, by its pure definition, can deliver experiences and interactions for students that are either not practical or not possible in the 'real world', it provides an unparalleled way to immerse and captivate our students. Virtual Reality helps students feel immersed in an experience, gripping their imagination and stimulating thought in ways not possible with traditional books, pictures or videos and it facilitates a far higher level of knowledge retention.

Enhancing and extending the learning experience is at the heart of what Virtual Reality can offer students.

Risks of VR headsets

i) Psychological risks

Negative impact on mental wellbeing

There will be an agreement in place regarding which students may not be suitable for wearing VR headsets, due to their mental health needs. This information will be added to the pupil list. Virtual reality is designed to be very realistic. This means that some more vulnerable young people might find it more difficult to tell the difference between what happens in the game and in reality. One side effect of using VR can be feeling disconnected from your body and is not recommended for anyone who has experienced symptoms of psychosis or disassociation.

Because VR is designed to be so realistic, it can feel strange to come out of the experience, students will not spend long time periods in headsets (no more than 15 minutes) as it might make them feel disconnected from their body, making them feel anxious or worried.

ii) Physiological risks

Immediately get the student to discontinue using the headset if any of the following symptoms are experienced: seizures; loss of awareness; eye strain; eye or muscle twitching; involuntary movements; altered, blurred, or double vision or other visual abnormalities;

dizziness; disorientation; impaired balance; impaired hand-eye coordination; excessive sweating; increased salivation; nausea; light-headedness; discomfort or pain in the head or eyes; drowsiness; fatigue; or any symptoms similar to motion sickness.

Experiencing physical injury

Teachers are to ensure that students remain seated and that the immediate area is free of any obstacles. There is also a risk of injury while wearing a headset as the wearer cannot see their surroundings. If they get up and move around, they could trip or fall on other items in the room.

Because of the way scenes move in VR, some people can feel motion sickness when using this technology. Using VR is an intense experience and using it for long periods of time could cause problems like eye strain - no more than 15 minutes at any one time must be spent in a headset.

Risk of electric shock

- Do not modify or open any of the components provided
- Do not use the product if any cable is damaged or any wires are exposed

Contagious conditions

The headset should be cleaned between each use with skin-friendly non-alcoholic antibacterial wipes and with a dry microfiber cloth for the lenses. To avoid transferring contagious conditions like conjunctivitis, do not share the headset with persons with contagious conditions, infections or diseases, particularly of the eyes, skin or scalp.

Skin irritation

The headset is worn next to the skin and scalp. Stop the student from using the headset in the event of swelling, itchiness, skin irritation or other skin reactions.

Seizures

Any student who has previously had a seizure, loss of awareness, or other symptom linked to an epileptic condition must not use the headset.

Repetitive strain injury

Using the device may make muscles, joints or skin hurt. If any part of the body become tired or sore while using the headset or its components**, usage must be stopped immediately**

Iii) Environmental risks

Experiencing unwanted contact/sharing private information

Our VR headsets do not allow any game play or chat. Some VR apps and games allow children to easily chat and play with people they don’t know. There is therefore no risk of

students sharing things like their name, where they go to school or photos of themselves. Location settings are also disabled.

Encountering harmful content

Internet restrictions are in place so that students do not see or hear things that are inappropriate, such as bad language, violence or sexual content.

Spending real money

Internet restrictions are in place so that students cannot make a purchase of real or virtual items or be open to ‘scammers.’

Appendix 6. Staff Declaration

Staff Declaration

I have read and understand the Digital Safety/ Social Media Policy and Acceptable Use of Property Policy and understand that inappropriate use may be considered to be misconduct or gross misconduct and may, after proper investigation, lead to a disciplinary sanction or dismissal.

I understand that, in certain circumstances, inappropriate use of Social Media may become a matter for police or social care investigations.

I understand that if I need any clarification regarding my use of Social Media, I can seek such clarification from any member of the Senior Leadership Team.

I confirm that I understand the Digital Safety/ Social Media Policy and Acceptable Use of Property Policy and have been given the opportunity to raise any queries or questions about the policy and have these satisfactorily addressed before signing this declaration.

SIGNED: ……..

PRINT NAME: ……

DATE: ……