Acceptable Use of Technology (AUP) for Staff and Volunteers

2022 – 2023

Staff Acceptable Use of Technology Policy

As a professional organisation with responsibility for safeguarding, all members of staff are expected to use The Discovery School IT systems in a professional, lawful, and ethical manner. To ensure that members of staff understand their professional responsibilities when using technology and provide appropriate curriculum opportunities for learners, they are asked to read and sign the staff Acceptable Use of Technology Policy (AUP).

Our AUP is not intended to unduly limit the ways in which members of staff teach or use technology professionally, or indeed how they use the internet personally, however the AUP will help ensure that all staff understand The Discovery School expectations regarding safe and responsible technology use and can manage the potential risks posed. The AUP will also help to ensure that school systems are protected from any accidental or deliberate misuse which could put the safety and security of our systems or members of the community at risk.

Policy Scope

1. I understand that this AUP applies to my use of technology systems and services provided to me or accessed as part of my role within The Discovery School both professionally and personally. This may include use of laptops, mobile phones, tablets, digital cameras, and email as well as IT networks, data and data storage, remote learning and online and offline communication technologies**.**

2. I understand that The Discovery School Acceptable Use of Technology Policy (AUP) should be read and followed in line with the school staff Code of Conduct and Online Safety Policy.

3. I am aware that this AUP does not provide an exhaustive list; all staff should ensure that technology use is consistent with The Discovery School ethos, staff behaviour and safeguarding policies, national and local education and child protection guidance, and the law.

Use of The Discovery School Devices and Systems

4. I will only use the equipment and internet services provided to me by The Discovery School for example The Discovery School provided laptops, tablets, mobile phones, and internet access, when working with learners.

5. I understand that any equipment and internet services provided by my workplace is intended for education purposes and for professional use and should only be accessed by members of staff.

Reasonable personal use of setting IT systems and/or devices by staff is not allowed. Only members of the Senior Management Team (SLT) and office staff can access the internet via their personal mobile phones. This is to allow them to remain contactable by staff who may be off-site or unwell.

6. Where I deliver or support remote learning, I will comply with The Discovery School remote learning AUP.

Data and System Security

7. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or securing/locking access.

    - I will use a 'strong' password to access school systems (a strong password has numbers, letters and symbols, with 8 or more characters, does not contain a dictionary word and is only used on one system).
    - I will protect the devices in my care from unapproved access or theft.
    - I will lock laptops when leaving the classroom or office. I will ensure that any digital documents taken off-site are stored on a protected storage device.

8. I will respect The Discovery School system security and will not disclose my password or security information to others.

9. I will not open any hyperlinks or attachments in emails unless they are from a known and trusted source. If I have any concerns about email content sent to me, I will report them to the IT Network Manager and a member of the SLT.

10. I will not attempt to install any personally purchased or downloaded software, including browser toolbars, or hardware without permission from the IT Network Manager.

11. I will ensure that any personal data is kept in accordance with the Data Protection legislation, including GDPR in line with the School's information security policies.

    - All personal data will be obtained and processed fairly and lawfully, only kept for specific purposes, held no longer than necessary and will be kept private and secure with appropriate security measures in place, whether used in the workplace, hosted online or accessed remotely.
    - Any data being removed from the school site, such as via email or on memory sticks, will be suitably protected. This may include data being encrypted by a method approved by the School.

12. I will not keep documents which contain school related sensitive or personal information, including images, files, videos, and emails, on any personal devices, such as laptops, digital cameras, and mobile phones.

13. I will not store any personal information on The Discovery School IT system, including school laptops or similar device issued to members of staff, that is unrelated to school activities, such as personal photographs, files or financial information.

14. I will ensure that The Discovery School owned information systems are used lawfully and appropriately. I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.

15. I will not attempt to bypass any filtering and/or security systems put in place by The Discovery School.

16. If I suspect a computer or system has been damaged or affected by a virus or other malware, I will report this to the Network Manager (Paul Robinson) as soon as possible.

17. If I have lost any school related documents or files, I will report this to the Network Manager (Paul Robinson) and School Data Protection Manager (Angela Alexander) as soon as possible.

18. Any images or videos of learners will only be used as stated in the school's Safe Use of Images policy and GDPR Policy. I understand images of learners must always be appropriate and should only be taken with school provided equipment and only be taken/published where parent/carers have given explicit written consent. Images will not be taken off-site.

Classroom Practice

19. I am aware of the expectations relating to safe technology use in the classroom, safe remote learning, and other working spaces as listed in the following policies:

    - Acceptable Use Policy
    - Safe Use of Images Policy
    - GDPR Policy
    - Online Safety Policy

20. I have read and understood The Discovery School Online Safety Policy which covers expectations for learners regarding mobile technology, social media and remote learning.

21. I will promote online safety with the learners in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create by:

    - exploring online safety principles as part of an embedded and progressive curriculum and reinforcing safe behaviour whenever technology is used.
    - creating a safe environment where learners feel comfortable to report concerns and say what they feel, without fear of getting into trouble and/or be judged for talking about something which happened to them online.

- involving the Designated Safeguarding Lead (DSL) (Tina Gobell) or a deputies (Jenny Baker and Amanda Lihou) as part of planning online safety lessons or activities to ensure support is in place for any learners who may be impacted by the content.
- make informed decisions to ensure any online safety resources used with learners is appropriate.

22. I will report any filtering breaches (such as access to illegal, inappropriate, or harmful material) to the DSL in line with the school's Online Safety and Child Protection Policies.

23. I will respect copyright and intellectual property rights; I will obtain appropriate permission to use content, and if videos, images, text, or music are protected, I will not copy, share, or distribute or use them.

Mobile Devices and Smart Technology

24. I will ensure that my use of mobile devices and smart technology is compatible with my professional role, does not interfere with my work duties and takes place in line with the staff Code of Conduct, the school's AUP and the law.

Online Communication, including Use of Social Media

25. I will ensure that my use of communication technology, including use of social media is compatible with my professional role, does not interfere with my work duties and takes place in line with the staff Code of Conduct, the school's AUP policy and the law.

- I will take appropriate steps to protect myself and my reputation online when using communication technology, including the use of social media.
- I will not discuss or share data or information relating to learners, staff, school business or parents/carers on social media.

26. My electronic communications with parents/carers will be transparent and open to scrutiny and will only take place within clear and explicit professional boundaries.

- I will ensure that all electronic communications take place in a professional manner via school approved communication channels and systems, such as a school email address, user account or telephone number.
- I will not share any personal contact information or details with learners, such as my personal email address or phone number.
- I will not add or accept friend requests or communications on personal social media with current or past learners and/or their parents/carers.
- If I am approached online by a current or past learner or parent/carer, I will not respond and will report the communication to my line manager and (Tina Gobell) Designated Safeguarding Lead (DSL).

- Any pre-existing relationships or situations that compromise my ability to comply with the AUP will be discussed with the Head Teacher or Deputy Head Teacher.

Policy Concerns

27. I will not upload, download, or access any materials which are illegal, such as child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act.

28. I will not attempt to access, create, transmit, display, publish or forward any material or content online that is inappropriate or likely to harass, cause offence, inconvenience, or needless anxiety to any other person.

29. I will not engage in any online activities or behaviour that could compromise my professional responsibilities or bring the reputation of The Discovery School into disrepute.

30. I will report and record concerns about the welfare, safety or behaviour of learners or parents/carers to the DSL in line with the School's Child Protection Policy.

31. I will report concerns about the welfare, safety, or behaviour of staff to a member of the SLT, in line with the allegations against staff policy.

Policy Compliance and Breaches

32. If I have any queries or questions regarding safe and professional practice online, either in school or off site, I will raise them with the Head teacher and DSL.

33. I understand that The Discovery School may exercise its right to monitor the use of its information systems, including internet access and the interception of emails, to monitor policy compliance and to ensure the safety of learners and staff. This monitoring will be proportionate and will take place in accordance with data protection, privacy, and human rights legislation.

34. I understand that if The Discovery School believes that unauthorised and/or inappropriate use of school systems or devices is taking place, the school may invoke its disciplinary procedures as outlined in the Staff Discipline and Conduct Policy.

35. I understand that if The Discovery School believes that unprofessional or inappropriate online activity, including behaviour which could bring the School into disrepute, is taking place online, the School may invoke its disciplinary procedures as outlined in the Staff Discipline and Conduct Policy.

36. I understand that if The Discovery School suspects criminal offences have occurred, the police will be informed.

I have read, understood and agreed to comply with The Discovery School Staff Acceptable Use of Technology Policy when using the internet and other associated technologies, both on and off site.

Name of staff member: ……

Signed: ……

Date (DDMMYY)……..

Appendix 1: Remote Learning

The Discovery School Staff Remote Learning AUP

The Remote Learning Acceptable Use Policy (AUP) is in place to safeguarding all members of school community when taking part in remote learning following any full or partial school closures.

Leadership Oversight and Approval

1. Remote learning will only take place using Microsoft Office Teams and Class DoJo.
    - These have been assessed and approved by the Senior Leadership Team (SLT).

2. Staff will only use school managed accounts with learners and 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 Tina Gobell, Designated Safeguarding Lead (DSL).
    - Staff will use work provided equipment.

3. Online contact with learners and/or parents/carers will not take place outside of the operating times as defined by SLT:
    - 8:00 a.m. to 4:00 p.m.

4. All remote lessons will be formally timetabled; a member of SLT will be able to drop in at any time.

5. Live-streamed remote learning sessions will only be held with approval and agreement from the Head Teacher.

Data Protection and Security

6. Any personal data used by staff and captured 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 school confidentiality expectations as outlined in the staff Code of Conduct.

8. All participants will be made aware that school systems record live teaching activity.

9. Staff will not record lessons or meetings using personal equipment.

10. Only members of the The Discovery School community will be given access to school systems.

11. Access to school systems will be managed in line with current IT security expectations.

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:
    - Disabling/limiting chat
    - Staff not permitting learners to share screens
    - Keeping meeting IDs private
    - The use of waiting rooms to manage privacy and confidential conversations
    - Staff will mute/disable learners' videos and microphones

14. Live sessions (including 1:1) will only take place with approval from a member of SLT. In the event that a live session is offered, then the parent must be in attendance, the session must be recorded and two members of staff must be present

15. A pre-agreed email detailing the session rules and expectations will be sent the parent/carer of 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.

16. Alternative approaches and/or access to a device will be provided to those who do not have access to their own.

Behaviour Expectations

17. Staff will model safe practice and moderate behavior, during online remote sessions as they would in the classroom.
18. All participants are expected to behave in line with existing school policies and expectations.
19. Staff will remind attendees of behaviour expectations and reporting mechanisms at the start of the session.
20. 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

21. Participants are encouraged to report concerns during remote sessions to a member of the SLT.
22. 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 a member of the SLT.
23. Inappropriate online behaviour will be responded to in line with existing policies e.g. acceptable use of technology, allegations against staff, anti-bullying and behaviour.
24. Any safeguarding concerns will be reported to Tina Gobell, Designated Safeguarding Lead, in line with our child protection policy.

Appendix 2:

Visitor and Volunteer Acceptable Use of Technology Policy

As a professional organisation with responsibility for safeguarding, it is important that all members of the community, including visitors and volunteers, are aware of our behaviour expectations and their professional responsibilities when using technology.

This AUP will help The Discovery School ensure that all visitors and volunteers understand the school's expectations regarding safe and responsible technology use.

Policy Scope

1. I understand that this Acceptable Use of Technology Policy (AUP) applies to my use of technology systems and services provided to me or accessed as part of my role within The Discovery School, both professionally and personally. This may include use of laptops, mobile phones, tablets, digital cameras, and email as well as IT networks, data and data storage, remote learning systems and communication technologies**.**

2. I am aware that this AUP does not provide an exhaustive list; visitors and volunteers should ensure that all technology use is consistent with the school's ethos, school behaviour and safeguarding policies, national and local education and child protection guidance, and the law.

Data and Image Use

3. I will ensure that any access to personal data is kept in accordance with Data Protection legislation, including GDPR.

4. I understand that I am not allowed to take images or videos of learners.

Classroom Practice

5. I am aware of the expectations regarding safe use of technology in the classroom and other working spaces, including appropriate supervision of learners.

6. I will support staff in reinforcing safe behaviour whenever technology is used on site and I will promote online safety with the children in my care.

7. I will immediately report any filtering breaches (such as access to illegal, inappropriate, or harmful material) to the Designated Safeguarding Lead (DSL) (Tina Gobell) in line with the school's Child Protection Policy.

8. I will respect copyright and intellectual property rights; I will obtain appropriate permission to use content, and if videos, images, text, or music is protected, I will not copy, share, or distribute or use it.

Use of Mobile Devices and Smart Technology

9. I understand that. Us eof personal device sis not permitted. Us eof of school device sis permitted via access to the guest WiFI for the day.

Online Communication, including the Use of Social Media

10. I will ensure that my online reputation and use of technology and is compatible with my role within the school. This includes my use of email, text, social media, social networking, gaming and any other personal devices or websites.
    - I will take appropriate steps to protect myself online as outlined in the Acceptable Use and Online Safety Policies.
    - I will not discuss or share data or information relating to learners, staff, school business or parents/carers on social media.
    - I will ensure that my use of technology and the internet will not undermine my role, interfere with my duties and will be in accordance with the school's expectation's and the law.

11. My electronic communications with learners, parents/carers and other professionals will only take place within clear and explicit professional boundaries and will be transparent and open to scrutiny.
    - All communication will take place via school approved communication channels
    - Communication will not take place via personal devices or communication channels such as via my personal email, social networking account or mobile phone number.
    - Any pre-existing relationships or situations that may compromise this will be discussed with the DSL (Tina Gobell)

Policy Compliance, Breaches or Concerns

12. If I have any queries or questions regarding safe and professional practice online either in school or off-site, I will raise them with the Designated Safeguarding Lead (Tina Gobell) or the a member of the SLT.

13. I will not upload, download, or access any materials which are illegal, such as child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act.

14. I will not attempt to access, create, transmit, display, publish or forward any material or content online that is inappropriate or likely to harass, cause offence, inconvenience, or needless anxiety to any other person.

15. I will not engage in any online activities or behaviour that could compromise my professional responsibilities or bring the reputation of the school into disrepute.

16. I understand that the school may exercise its right to monitor the use of school information systems, including internet access and the interception of emails, to monitor policy compliance and to ensure the safety of learners, staff and visitors/volunteers. This monitoring will be proportionate and will take place in accordance with data protection, privacy, and human rights legislation.

17. I will report and record concerns about the welfare, safety or behaviour of learners or parents/carers to the Designated Safeguarding Lead (Tina Gobell) in line with the school's Child Protection Policy.

18. I will report concerns about the welfare, safety, or behaviour of staff to the Head Teacher or Deputy Head Teacher, in line with the allegations against staff policy.

19. I understand that if the school believes that unauthorised and/or inappropriate use, or unacceptable or inappropriate behaviour is taking place online, the school may invoke its procedures outlined in the Staff Discipline and Conduct Policy

20. I understand that if the school suspects criminal offences have occurred, the police will be informed.

I have read, understood and agreed to comply with The Discovery School Visitor/Volunteer Acceptable Use of Technology Policy when using the internet and other associated technologies, both on and off site.

Name of visitor/volunteer: ……..……

Signed: …….....

Date (DDMMYY)…….....

Appendix 3:

Wi-Fi Acceptable Use Policy

As a professional organisation with responsibility for children's safeguarding it is important that all members of the school community are fully aware of the school boundaries and requirements when using the school's Wi-Fi systems, and take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft.

This is not an exhaustive list, and all members of The Discovery School community are reminded that technology use should be consistent with our ethos, other appropriate policies, and the law.

1. The Discovery School provides Wi-Fi for the school community and allows access for educational purposes only.

2. I am aware that The Discovery School will not be liable for any damages or claims of any kind arising from the use of the wireless service. The School takes no responsibility for the security, safety, theft, insurance, and ownership of any device used within the school premises that is not the property of the school.

3. The use of technology falls under The Discovery School Acceptable Use of Technology Policy (AUP), online safety policy and behaviour policy, which all learners/staff/visitors and volunteers must agree to and comply with.

4. The Discovery School reserves the right to limit the bandwidth of the wireless service, as necessary, to ensure network reliability and fair sharing of network resources for all users.

5. The Discovery School owned information systems, including Wi-Fi, must be used lawfully; I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.

6. I will take all practical steps necessary to make sure that any equipment connected to the school service is adequately secure, such as up-to-date anti-virus software, systems updates.

7. The Discovery School wireless service is not secure, and the School cannot guarantee the safety of traffic across it. Use of the school's wireless service is done at my own risk. By using this service, I acknowledge that security errors and hacking are an inherent risk associated with any wireless network. I confirm that I knowingly assume such risk.
8. The Discovery School accepts no responsibility for any software downloaded and/or installed, email opened, or sites accessed via the school's wireless service's connection to the internet. Any damage done to equipment for any reason including, but not limited to, viruses, identity theft, spyware, plug-ins or other internet-borne programs is my sole responsibility; and I indemnify and hold harmless the school from any such damage.

9. I will respect system security; I will not disclose any password or security information that is given to me. To prevent unauthorised access, I will not leave any information system unattended without first logging out or locking my login as appropriate.

10. I will not attempt to bypass any of the school's security and filtering systems or download any unauthorised software or applications.

11. My use of school's Wi-Fi will be safe and responsible and will always be in accordance with the school's AUP and the law including copyright and intellectual property rights. This includes the use of email, text, social media, social networking, gaming, web publications and any other devices or websites.

12. I will not upload, download, access or forward any material which is illegal or inappropriate or may cause harm, distress or offence to any other person, or anything which could bring The Discovery School into disrepute.

13. I will report any online safety concerns, filtering breaches or receipt of inappropriate materials to the Designated Safeguarding Lead (Tina Gobell) as soon as possible.

14. If I have any queries or questions regarding safe behaviour online, I will discuss them with Designated Safeguarding Lead (Tina Gobell) or the Head Teacher.

15. I understand that my use of the school's Wi-Fi may be monitored and recorded to ensure policy compliance in accordance with privacy and data protection legislation. If the school suspects that unauthorised and/or inappropriate use or unacceptable or inappropriate behaviour may be taking place, then the school may terminate or restrict usage. If the school suspects that the system may be being used for criminal purposes, the matter will be brought to the attention of the relevant law enforcement organisation.

I have read, understood and agreed to comply with The Discovery School Wi-Fi acceptable Use Policy.

Name ……..…...

Signed: …….....Date (DDMMYY)……...

Appendix 4:

Additional information and guides on specific platforms can be found at:

- https://coronavirus.lgfl.net/safeguarding
- https://swgfl.org.uk/resources/safe-remote-learning/video-conferencing-for-kids-safeguarding-and-privacy-overview/

Further information and guidance for SLT and DSLs regarding remote learning:

- Local guidance:
  - Kelsi:
    - Guidance for Full Opening in September
    - Online Safety Guidance for the Full Opening of Schools
  - The Education People: Covid-19 Specific Safeguarding Guidance and Resources
    - 'Safer remote learning during Covid-19: Information for School Leaders and DSLs'
    -

- National guidance:
  - DfE:
    - 'Safeguarding and remote education during coronavirus (COVID-19)
  - SWGfL:
    - Safer Remote Learning
  - LGfL: Coronavirus Safeguarding Guidance
  - NSPCC:
    - Undertaking remote teaching safely
  - Safer Recruitment Consortium:
    - 'Guidance for safer working practice for those working with children and young people in education settings Addendum' April 2020