Acceptable Use of Technology for Staff, Visitors and Volunteers

Included in this policy are:

- **Staff Acceptable Use of Technology Policy (AUP)**
- **Wi-Fi Acceptable Use Policy (AUP)**
- **Staff Remote/Online Learning (AUP)**

Key Details

Designated Safeguarding Lead (s): Tina Gobell, Headteacher

Named Governor with lead responsibility: Annabel Cornall, Chair of Governors

Date written/updated: September 2025

Date of next review: September 2026

This policy will be reviewed **at least** annually. It will also be revised following any concerns and/or updates to national and local guidance or procedures.

Staff Acceptable Use of Technology Policy (AUP)

As a professional organisation with responsibility for safeguarding, all members of staff are expected to use 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 children 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 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 Acceptable Use of Technology Policy (AUP) applies to my use of technology systems and services, either provided to me by the school or accessed by me as part of my role within The Discovery School professionally and personally, both on and offsite. This may include my use of devices such as laptops, mobile phones, tablets, digital cameras, as well as IT systems and networks, email. data and data storage, remote learning systems and communication technologies**.**

2. I understand that The Discovery School Acceptable Use of Technology Policy (AUP) should be read and followed in line with The Discovery School Child Protection policy staff code of conduct.

3. I am aware that this AUP does not provide an exhaustive list; all staff should ensure that technology use is consistent with the school ethos, The Discovery School 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 school provided laptops, tablets, mobile phones and internet access, when working with children.

5. I understand that any equipment and internet services provided by my workplace is intended for education purposes and/or professional use and should only be accessed by members of staff. Reasonable personal use of setting IT systems and/or devices by staff is allowed, however this use is at the Headteacher's discretion and can be revoked at any time. Acceptable uses of the school systems could be:

    - Using personal mobile phone, in the staffroom to check emails or messages

- Using the school computers to word process documents.

Data and system security

6. 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.
    - It is good practice to change these passwords every 3-6 months for high-risk accounts, such as finance and yearly for other passwords.
    - I will protect the devices in my care from unapproved access or theft. Devices should not be left in vehicles overnight and should be stored safely and securely if being used at home.
    - 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.

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

8. 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 both the Headteacher and IT System Manager, Paul Robinson.

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

10. I will ensure that any personal data is kept in accordance with the Data Protection legislation, including UK GDPR in line with the school 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.
    - Any data being shared online, such as via cloud systems or artificial intelligence tools (AI), will be suitably risk assessed and approved by the school Data Protection Officer and Senior Leadership team prior to use to ensure it is safe and legal.

11. 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.

12. I will not store any personal information on the 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.

13. I will ensure that 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.

14. I will not attempt to bypass any filtering and/or security systems put in place by the school.

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

16. If I have lost any school related documents or files, I will report this to the ICT Support Manager (Paul Robinson) and The Discovery School Data Protection Officer (Angela Alexander) as soon as possible.

17. I understand images of children must always be appropriate and should only be taken with school provided equipment and only be taken/published where children and/or parent/carers have given explicit written consent.

Classroom practice

18. I understand that it is part of my roles and responsibilities to ensure that appropriate filtering and monitoring is implemented by The Discovery School as detailed in The Discovery School Child Protection policy, and as discussed with me as part of my induction and/or ongoing safeguarding and child protection staff training.

19. If there is failure in the filtering software or abuse of the filtering or monitoring systems, for example, I witness or suspect accidental or deliberate access to illegal, inappropriate or harmful material, I will report this to the DSL and IT Support Manager, in line with The Discovery School Child Protection policy.

20. 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 Discovery School child protection policy, and remote learning AUP.

21. I am aware that generative artificial intelligence (AI) tools may have many uses which could benefit our school community. However, I also recognise that AI tools can also pose risks, including, but not limited to, bullying and harassment, abuse and exploitation (including child sexual abuse), privacy and data protection risks, plagiarism and cheating, and inaccurate, harmful and/or biased material. Additionally, its use can pose moral, ethical and legal concerns if not carefully managed. As such, I understand that:
    - AI tools are only to be used responsibly and ethically, and in line with our school Child Protection, Data Protection, and staff Code of Conduct expectations.
    - A risk assessment will be undertaken, and written approval will be sought from the Senior Leadership Team prior to any use of AI tools, for example if used in the classroom, or to support lesson planning.
    - A Data Protection Impact Assessment (DPIA) will always be completed prior to any use of AI tools that may be processing any personal, sensitive or confidential data and use will only occur following approval from the DPO.

- I am required to critically evaluate any AI-generated content for accuracy, bias, and appropriateness before sharing or using it in educational contexts.
- AI must not be used to replace professional judgement, especially in safeguarding, assessment, or decision-making involving children.
- Only approved AI platforms may be used with children. Children must be supervised when using AI tools, and I must ensure age-appropriate use and understanding prior to use.
- Any misuse of AI will be responded to in line with relevant school policies, including but not limited to, Data Security, Anti-bullying, staff Code of Conduct, Behaviour and Child Protection.

22. I will promote online safety with the children 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 children 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 deputy (Jenny Oakes and Jane Wilce Cordner) as part of planning online safety lessons or activities to ensure support is in place for any children who may be impacted by the content.
    - Informing the DSL and/or Senior Leadership team if I am teaching topics which could create unusual activity on the filtering logs, or if I believe the filtering system is placing unreasonable restrictions on teaching, learning or administration.
    - make informed decisions to ensure any online safety resources used with children is appropriate.

23. I will respect copyright and intellectual property rights and ensure my use of online platforms and tools is safe, legal and ethical; I will obtain appropriate permission to use content, and if videos, images, text, or music are protected, I will not copy, share, misuse, plagiarise, or distribute them.

Mobile devices and smart technology

24. I have read and understood the school mobile and smart technology and Child Protection policies which addresses use by children and staff.

25. 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 and the school mobile technology policy and the law

Online communication, including use of social media

26. 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 child protection policy, staff code of conduct, Staff AUP and the law.

27. As outlined in the staff code of conduct and school social media policy:

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

28. My electronic communications with current and past children and 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 and/or provided 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 children, 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 children's and/or their parents/carers.
    - If I am approached online by a current or past children or parents/carers, 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 or other relevant policies will be discussed with the DSL and/or headteacher.

Policy concerns

29. 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.

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

31. 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.

32. I will report and record any concerns about the welfare, safety or behaviour of children or parents/carers online to the DSL in line with the school child protection policy.

33. I will report concerns about the welfare, safety, or behaviour of staff online to the headteacher, in line with school child protection policy and the allegations against staff policy.

Policy Compliance and Breaches

34. If I have any queries or questions regarding safe and professional practise online, either in school or off site, I will raise them with the DSL and the headteacher.

35. I understand that the school may exercise its right to monitor the use of its devices information systems to monitor policy compliance and to ensure the safety of children and staff. This includes monitoring all school provided devices and school systems and networks including school provided internet access, whether used on or offsite and may include the interception of messages and emails sent or received via school provided devices, systems and/or networks. This monitoring will be proportionate and will take place in accordance with data protection, privacy, and human rights legislation.

36. I understand that if the school believe that unauthorised and/or inappropriate use of school devices, systems or networks is taking place, the school may invoke its disciplinary procedures as outlined in the staff code of conduct.

37. I understand that if the school believe 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 code of conduct.

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

The Discovery School Wi-Fi Acceptable Use Policy

As a professional organisation with responsibility for children's safeguarding it is important that all members of The Discovery School community are fully aware of The Discovery School boundaries and requirements when using The Discovery School 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 education use 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 Discovery 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 Discovery School.

3. The use of technology falls under The Discovery School Acceptable Use of Technology Policy (AUP), Child Protection Policy (online safety included in this) and behaviour policy which all 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 Discovery 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 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 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 Discovery 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 Discovery School security and filtering systems or download any unauthorised software or applications.

11. My use of The Discovery School Wi-Fi will be safe and responsible and will always be in accordance with The Discovery School 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.

15. I understand that my use of The Discovery School 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 Discovery School may terminate or restrict usage. If The Discovery 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.

The Discovery School Staff Remote/Online Learning (AUP)

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

Leadership oversight and approval

1. Remote/online learning will only take place using Microsoft Office Teams and Class DoJo.
    - Microsoft Office Teams and Class DoJo have been assessed and approved by the headteacher and the Senior Leadership Team (SLT).
2. Staff will only use school managed approved professional accounts with children and parents/carers.
    - Use of any personal accounts to communicate with children 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 where possible**,** for example, a school laptop, tablet, or other mobile device.
3. Online contact with children **or** parents/carers will not take place outside of the operating times as defined by SLT:
    - 8am to 4pm

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

5. Live-streamed remote/online 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/online learning and any other online communication will take place in line with current school confidentiality expectations as outlined in The Discovery School Staff Code of Conduct.
8. All participants will be made aware that Microsoft Office Teams records 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.

    - Access to The Discovery School systems will be managed in line with current IT security expectations.

Session management

11. Staff will record the length, time, date, and attendance of any sessions held.

12. Appropriate privacy and safety settings will be used to manage access and interactions. This includes:
13. 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. If 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 to 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.

17. Alternative approaches and/or access will be provided to those who do not have access, including the loan of equipment.

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 school policies and expectations.
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 to member of the SLT.
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 any member of the SLT.

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. Any safeguarding concerns will be reported to Tina Gobell, Designated Safeguarding Lead, in line with our child protection policy.

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

- LGfL: Safeguarding Considerations for Remote Learning
- SWGfL: Which Video Conference platform is best?

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

- Local guidance:
  - Kelsi:
    - 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
  - NSPCC: Undertaking remote teaching safely
  - Safer Recruitment Consortium: Guidance for safer working practice

Please sign and return to the school office once you have read the policy and appendices.

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)……..

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

Name ……..…..

Signed: Date (DDMMYY)

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

Name of staff member: ……

Signed: ……