Online Safety Policy and Guidance

December 2024

CONTENTS

DOCUMENT CONTROL

Who is this policy for?

This policy applies to all Delta Members, Trustees, staff, students, AAB members, visitors and contractors.

This Policy Statement

The aim of this policy is to protect the interests and safety of the whole Delta community and to highlight the range of risks associated with the use of ICT and related technologies.

Protective marking

Not protectively marked.

Review date

This policy will next be reviewed before December 2027.

Revision History

REVISION	DATE	DESCRIPTION	AUTHOR
1	June 2021	Revised policy approved by the Audit and Risk Committee. Key changes summary: • Terminology change as per DfE guidance. • Phishing section added (section 15). • Additional detail added to social media section which addresses the use of Instagram, WhatsApp and TikTok (section 9.6). • Remote access section updated to include requirements around MFA (Multi Factor Authentication) and VPN (Virtual Private Network) (Section 11). • Acceptable Use Agreement for students updated (Appendix 2). • Trust or Academy loaned device agreement added (Appendix 2b).	
2	December 2024	Policy revised.	Emma Mayor/Amie Wagstaff

1. INTRODUCTION

1.1 Delta Academies Trust's (Delta) intention in publishing an Online Safety Policy is not to impose restrictions that are contrary to Delta's established culture of openness, trust and integrity. This policy, supported by the acceptable use agreements for Trustees, Members, staff, Academy Advisory Body (AAB) Members, visitors, volunteers and students, is designed to protect the interests and safety of the whole Delta community. All users need to be aware of the range of risks associated with the use of ICT and related technologies.

2. ROLES AND RESPONSIBILITIES

2.1 The Principal/Head of Academy is responsible for ensuring that the policy and associated practices are embedded and monitored in Academies. Executive Leadership Team (ELT) members are responsible for the implementation of this policy in the Core Team.

2.2 The Principal/Head of Academy may nominate an Online Learning or Online Safety Lead in a standalone role or as part of their wider leadership remit. If no Online Learning or Online Safety Lead is nominated, the Principal/Head of Academy will be deemed to be responsible for online safety/learning in their Academy.

2.3 All elements of this policy apply to Members, Trustees, AAB Members, students, staff, contractors, consultants, and other workers at Delta, including all personnel affiliated with third parties. It also applies to members of the public who use or connect to Delta equipment. This policy applies to all equipment that is owned or leased by Delta and the use of other devices to access the Delta network.

2.4 Any employee found to have violated any aspect of this policy and guidance may be subject to disciplinary action under Delta's Disciplinary Procedure, up to and including termination of employment. All staff will be asked to sign an Acceptable Use Agreement as part of their induction process - please see **Appendix 1.**

2.5 For safeguarding and consistency for learning purposes, it is the responsibility of all staff and students to ensure that all online communications is through their designated Delta email address.

3. SCOPE

3.1 This policy and guidance applies to both fixed and mobile internet technologies provided by Delta or an Academy (such as PCs, laptops, mobile phones, internet WIFI dongles, tablets, webcams, whiteboards, voting systems, digital video equipment,

etc.) and technologies owned by students and staff, but brought onto Academy premises or connected to the Delta network (such as laptops, mobile phones, camera phones, PDAs and portable media players, etc.)

3.2 This policy applies to any online platforms endorsed by the Trust to expand and enhance learning. (e.g. the Office365 Suite).

3.3 These technologies are to be used for Trust and learning purposes in serving the interests of our students and staff in the course of normal or enhanced operations.

4. ONLINE SAFETY IN THE CURRICULUM

4.1 Delta has a framework for teaching internet skills in Computing/ Life (PHSE) lessons.

4.2 Delta provides opportunities within a range of curriculum areas to teach about online safety.

4.3 Educating students on the dangers of technologies that may be encountered outside Delta is carried out both informally when opportunities arise and formally as part of the online safety curriculum.

4.4 Students are made aware of the relevant legislation when using the internet such as data protection and intellectual property, which may limit what they want to do but also serves to protect them.

4.5 Students are taught about copyright and respecting other people's information, images, etc. through discussion, modelling and activities.

4.6 Students are made aware of the impact of online bullying and of how to seek help if they are affected by these issues. Students are also made aware of where to seek advice or help if they experience problems when using the internet and related technologies i.e. Learning Mentors, parent/carer, teacher/ trusted staff member, or an organisation such as Childline/Child Exploitation and Online Protection (CEOP) report abuse button.

4.7 Students are taught to evaluate materials critically and to learn good searching skills through cross curricular teacher models, discussions and via the Computing curriculum.

4.8 Students with Additional Needs

4.8.1 Delta endeavours to ensure that each Academy creates a consistent message with parents of all students. However, staff are aware that some students may require additional teaching including reminders, prompts and

further explanation to reinforce their existing knowledge and understanding of online safety issues.

4.8.2 Where a student has additional needs in respect of social understanding, careful consideration should be given to group interactions when raising awareness of online safety. Internet activities must be planned and well managed for all children and young people and with particular care for children with these additional needs.

4.9 Parental Involvement

4.10 Parents/ carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to the Academy. Please see **Appendix 2 and 2B.**

4.11 Parents/ carers are required to make a decision as to whether they consent to images of their child being taken/ used in the public domain (e.g. on an Academy website). Please see **Section 10.**

4.12 The Academy disseminates information to parents relating to online safety where appropriate in the form of:

4.12.1 Information and celebration evenings;

4.12.2 Posters;

4.12.3 Website/ Online Learning Platform postings and learning platform training;

4.12.4 Newsletter items; and

4.12.5 Online, text message and email communication.

5. PASSWORD SECURITY

All users are responsible for implementing password security in all aspects of creating, protecting and managing passwords. Passwords for Delta systems must be created and managed in accordance with this policy. See **Appendix 3** for guidance.

5.1 Password Disclosure

5.1.1 Users must not disclose their passwords to anyone.

5.1.2 Users must not write their passwords down under any circumstances.

5.1.3 Unauthorised password disclosure is deemed a serious security matter and may be dealt with under Delta's Disciplinary Procedure and Acceptable Use Agreement, up to and including termination of employment for staff.

5.2 Shared Passwords

5.2.1 There may be rare occasions when it is necessary to share a common password between more than one user, if having individual usernames and passwords is operationally unacceptable, such as where the sharing of equipment is required, and the logout and login times required to swap users are unacceptable.

5.2.2 Any such arrangement **must** be authorised by ICT.

5.2.3 All access to applications through the Microsoft 365 Platform including email, will be gained through the use of individual logins, which will have to be entered by each user independently.

5.3 Data Security

5.3.1 The accessing of Academy data is something that Delta takes very seriously.

5.3.2 Any data shared with an external body must be subject to a data sharing agreement approved by the Data Protection Officer via dpo@deltatrust.org.uk.

5.3.3 Staff must be made aware of their responsibilities when accessing Academy data.

5.3.4 They **must** not:

5.3.4.1 Take copies of the data;

5.3.4.2 Allow others to view the data (unless this is required for business purposes);

5.3.4.3 Edit the data unless specifically requested to do so by the Principal/Head of Academy;

5.3.4.4 Leave the Management Information System (MIS) or other programmes/applications open for students to view;

5.3.4.5 Leave their workstations unlocked when leaving the classroom;

5.3.4.6 Allow a student to use the teacher's PC; and

5.3.4.7 Share staff passwords or store passwords insecurely.

6. ACCEPTABLE USE AGREEMENTS

Effective security is a team effort involving the participation and support of every Delta employee, student and partner who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

6.1 General Use and Ownership

6.1.1 While the Delta Core Information Technology Services team (CITS) wishes to provide a reasonable level of privacy, users should be aware that the data or emails they create on the Delta systems or that reference Delta remain the property of the Trust. Because of the need to protect the Delta network, management cannot guarantee the confidentiality of information stored on any network device belonging to Delta or Delta systems e.g. Office365.

6.1.2 Staff are responsible for exercising good judgment regarding the reasonableness of personal use. If there is any uncertainty, staff should consult their supervisor or manager.

6.1.3 For security and network maintenance purposes, authorised individuals within Delta may monitor equipment, systems and network traffic at any time.

6.1.4 Delta reserves the right to audit networks and systems on a periodic basis.

6.2 Acceptable Use Agreements

Users should sign the relevant acceptable use agreement in **Appendices 1, 2 and 2B.**

6.3 Unacceptable Use

The activities listed in **Appendix 4** are prohibited.

7. MANAGING THE INTERNET SAFELY

7.1 Delta monitors Internet use from all computers and devices connected to the corporate network. For all traffic, the monitoring system must record the source IP Address, the date, the time, the protocol, and the destination site or server. Where possible, the system should record the User ID of the person or account initiating the traffic. Internet Use records must be preserved for ninety (90) days.

7.2 Core Information Technology Services (CITS) members may access all reports and data if necessary to respond to a security incident. Internet Use reports that identify specific users, sites, teams, or devices will only be made available to

associates outside the CITS upon written or email request to CITS from a management team member (with authorisation from ELT or the Director of HR). Further guidance on managing the internet safely is provided in **Appendix 5.**

8. MANAGING EMAIL AND THE FULL MICROSOFT 365 PLATFORM

8.1 The Microsoft 365 Platform (Outlook, Teams etc.) which hosts the Delta email system must not to be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, hair colour, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin. Staff or students who receive any emails with this content should report the matter immediately. Staff should report this to their Line Manager and students should report this to their Learning Manager or relevant member of SLT. Any breach of this online safety policy may be dealt with under the acceptable use agreements for all users, the Delta Disciplinary Procedure, up to and including termination of employment for staff, the relevant section of the Care, Support, Guidance and Behaviour Policy for pupils/students and the Code of Conduct for Members, Trustees and AAB members .

8.2 Personal Use

Using a reasonable amount of Delta Academies Trust resources for personal emails is acceptable, but non-work related email must be saved in a separate folder from work related email.

Sending chain letters or joke emails from a Delta email account is prohibited. Virus or other malware warnings and mass mailings from Delta accounts must be approved by CITS before sending. Designated user groups are set up for the receipt of multi-target communication.

8.3 Monitoring

Delta staff or students shall have no expectation of privacy in anything they store, send or receive on the Trust's email or wider online learning platforms. Delta may monitor messages without prior notice. Delta is not obliged to monitor email messages.

8.4 Email Forwarding Policy

Delta staff and secondary students are provided with a Delta email account. Staff and secondary students are not permitted to use personal email accounts for Delta purposes. Unless approved by an employee's Line Manager or Learning

Manager/relevant member of SLT, Delta email will not be automatically forwarded to an external email address.

9. SOCIAL NETWORKING

9.1 Delta does not discourage staff and students from using such services in their own time. However, all should be aware that Delta will take seriously any occasions where the services are used inappropriately. If online bullying or harassment is found to have taken place, these will be dealt with in accordance with the Acceptable Use Agreements, Delta Harassment and Bullying policy for staff, the relevant section of the Care, Support, Guidance and Behaviour Policy for pupils/students and the Code of Conduct for Members, Trustees and AAB members.

9.2 It is important to recognise that there are also issues regarding the appropriateness of some content, contact, culture and commercialism. To this end, we encourage staff and students to think carefully about the way that information can be added and removed by all users, including themselves, from these sites. Additional guidance for both staff and students is included in **Appendix 5.**

9.3 Any serious misuse of Social Networking sites will be dealt with in accordance with the Delta Disciplinary policy.

9.4 Guidance is provided below in respect of Facebook, Twitter, Instagram, WhatsApp and TikTok. The same principles should be applied to other social networking sites. This list is not exhaustive.

9.5 Twitter

Delta Academies may use Twitter social networking as method of communication with stakeholders. This communication is permitted by Delta providing it adheres to the following guidelines:

9.5.1 The Principal/Head of Academy is responsible for the content of the Academy Twitter feed.

9.5.2 The Twitter feed must be used for Academy purposes only. The content must be appropriate and considered and must not contain reference to any personal/political views.

9.5.3 Access to an Academy Twitter account will be managed by the Principal/Head of Academy with an authorised user list available to Delta on request.

9.5.4 An administration account for all Academy Twitter feeds must be submitted to Delta CITS upon request.

9.5.5 Inappropriate content posted via Twitter will result of suspension of the account and control of the account will be taken by Delta CITS.

9.6 Facebook and Instagram

9.6.1 Delta Academies are only permitted to use Facebook and/or Instagram accounts as a method of communication with stakeholders or with prior authorisation from the Information Governance Steering Group. Corporate marketing accounts will only be allowed with ELT authorisation.

9.6.2 Staff may use Facebook/Instagram in their own time using their own IT assets. However:

9.6.2.1 Under no circumstances should students or ex-students under the age of 18 be accepted as a friend/follower. Failure to follow this will result in disciplinary action being taken. If a child requests a member of staff as a friend/follower then the child's parents must be informed. This should be reported to SLT who will arrange for parents to be contacted;

9.6.2.2 Staff are asked to use extreme caution if a parent makes contact through Facebook or Instagram. In the event of communicating with a parent or adult associated with a child who attends the school, an employee must not make any comments about students, staff or parents;

9.6.2.3 Any statements or status/post remarks made by staff must not contain any comments about Delta, the Academy, staff, parents or students.

9.7 WhatsApp, TikTok and Other Social Media Platforms

9.7.1 Staff may use the above/other social networking sites in their own time using their own IT assets. However:

9.7.1.1 Under no circumstances should students or ex-students under the age of 18 be accepted as followers or contacts. Failure to follow this will result in disciplinary action being taken. If a child requests to follow or communicate with a member of staff via these methods then the child's parents must be informed.

9.7.1.2 Staff are asked to not make contact with parents or students using these methods.

9.7.1.3 Any content or correspondence must not contain any comments about Delta, the Academy, staff, parents or students.

9.7.1.4 For any social media usage requests outside of this policy, please contact the Principal/Head of Academy or ICT department in the first instance.

10. SAFE USE OF IMAGES

10.1 Digital images are easy to capture, reproduce and publish and also to misuse. It is not always appropriate to take or store images of any member of the Academy community or public, without first seeking consent and considering the images for appropriateness.

10.2 With the written consent of parents (on behalf of pupils/students) and staff, Academies may permit the appropriate taking of images and recordings by staff and pupils/students with Academy equipment.

10.3 **Staff** are not routinely permitted to use personal digital equipment, such as mobile phones and cameras, to record images of students; this includes when on field trips. However, with the express permission of the Principal/Head of Academy, images can be taken, provided they are transferred immediately and solely to the Academy's network and deleted from the staff device. IT support may be required to complete this.

10.4 **Pupils and students** are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of others; this includes when on field trips. However, with the express permission of the Principal/Head of Academy, images can be taken provided they are transferred immediately and solely to the Academy's network and deleted from the student's device.

10.5 **Pupils/students** are permitted to use personal digital equipment to access the online learning platforms and their wider functionality for directed learning activities. They may take images and recordings of their own work and upload these to the learning platform.

10.6 Consent of Adults Who Work at the Academy

Permission to use images of all staff who work at the Academy should be sought on induction and a copy retained in the individual's personnel file.

10.7 Publishing Students' Images and Work

10.7.1 On a child's entry to the Academy, parents/carers will be asked to give permission to use their child's work/photos in the following ways:

10.7.1.1 on the Academy or Trust website;

10.7.1.2 on the Office365 environment e.g. learning platform, Teams;

10.7.1.3 in the Academy prospectus and other printed publications that the Academy may produce for promotional purposes;

10.7.1.4 recorded/ transmitted on a video or webcam;

10.7.1.5 in display material that may be used in the Academy's/Trust's communal areas;

10.7.1.6 in display material that may be used in external areas e.g. an exhibition promoting the Academy/Trust; and

10.7.1.7 general media appearances, e.g. local/national media/press releases sent to the press highlighting an activity (sent using traditional methods or electronically).

10.7.2 This consent form (please see **Appendix 4** of the Data Protection Policy) is considered valid for the entire period the child attends the Academy unless there is a change in the child's circumstances where consent could be an issue, e.g. divorce of parents, custody issues, etc.

10.7.3 In general terms, if a student is aged 13 or over, then we will assume that they have the competence to understand and provide or withdraw consent to the use of their data. Each student and the level of their understanding must be judged on a case-by-case basis.

10.7.4 Parents/carers (or students if aged 13 or over or are otherwise deemed competent to give consent) may withdraw permission, in writing, at any time. Consent has to be given by the person with parental responsibility or the student themselves (if aged 13 or over or are otherwise deemed competent to give informed consent) to be valid.

10.7.5 Students' full names will not be published alongside their image. Email and postal addresses of students will not be published. Before posting student work on the Internet, a check needs to be made to ensure that permission has been given for work to be displayed. No photos should be uploaded to website or put in any publications without prior checking with the Principal/Head of Academy or nominated responsible person at the Academy.

10.7.6 Only Delta or the nominated responsible person at the Academy has authority to upload images to the Academy website**. If links to YouTube are**

provided, a disclaimer must state that this link is to an external website and that Delta is not responsible for the content of external sites.

10.8 Storage of Images

10.8.1 Images/films of children are stored on the Academy's network and Office365 environment.

10.8.2 Students and staff are not permitted to use personal portable media for storage (e.g. USB sticks) without the express permission of the Director of ICT. Students and staff should use Office365 OneDrive for all storage.

10.8.3 Rights of access to this material are restricted to the teaching staff and students within the confines of the Academy network/Online Learning Platform.

10.9 CCTV

Please see the Delta Data Protection Policy.

10.10 Microsoft Teams and Video Conferencing Platforms

Video conferencing can provide valuable leaning opportunities but the associated risks need to be carefully considered and managed. **Appendix 6** provides specific guidance in respect of the use of video conferencing by Academies.

11. REMOTE ACCESS

11.1 At Delta, the Office365 environment can be accessed via devices which have Multi Factor Authentication (MFA). This applies to all devices connecting to the Office365 suite at Delta, regardless of ownership.

11.2 The Delta network is only accessible to approved devices. Networks can be accessed from home with a Delta Virtual Private Network (VPN). The issue of VPNs is authorised on a needs basis. Requests to ICT will be discussed with the Principal/Head of Academy or ELT.

11.3 Mobile computing and storage devices include, but are not limited to: laptop computers, mobile phones, WIFI dongles, plug-ins, Universal Serial Bus (USB) port devices, Compact Discs (CDs), Digital Versatile Discs (DVDs), flash drives, modems, handheld wireless devices, wireless networking cards, and any other existing or future mobile computing or storage device, either personally owned or Delta owned, that may connect to or access the information systems at Delta.

11.4 A risk analysis for each new media type must be conducted by the ICT department and documented prior to its use or connection to the network at Delta.

12. MOBILE TECHNOLOGIES, INCLUDING REMOVABLE MEDIA DEVICES

12.1 Students and staff are not permitted to use personal portable media for storage (e.g. USB sticks) without the express permission of the Director of ICT. Students and staff should use their online cloud storage through OneDrive for all storage.

12.2 Removable media devices, including laptops, mobile phones, tablets and USB memory sticks are particularly vulnerable to loss and theft due to their size and portability. Users must take all reasonable precautions to prevent a security breach. Approval for access to, and use of, mobile computing and removable media devices must be given by CITS. Should access to, and use of, mobile computing and removable media devices be approved, the following sections apply and must be adhered to at all times.

12.3 Special care **must** be taken to physically protect the removable media device and stored information from loss, theft or damage. Anyone using removable media devices to transfer information must consider the most appropriate way to transport the device and be able to demonstrate that they took reasonable care to avoid damage or loss.

12.4 Only information that is authorised and necessary to be transferred should be saved on to the removable media device. Users should note that information that has been deleted can still be retrieved.

12.5 Removable media devices **must not** be used for archiving or storing records as an alternative to other storage equipment.

12.6 Non-Delta owned removable media devices **must not** be used to store any information used to conduct official Delta business, and **must not** be used with any Delta owned or leased IT equipment unless authorised by Delta Core IT Services.

12.7 Further detailed guidance is provided in **Appendix 7.**

12.8 It should be noted that if a user loses or has a mobile device/tablet stolen which contains unencrypted personal data owned by Delta, they must contact the Trust Data Protection Officer immediately via dpo@deltatrust.org.uk .

12.9 Inappropriate Material

12.9.1 All users must be made aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the Online Safety Co-ordinator. The Online Safety Coordinator must record the incident on the online safety log. Please see

Appendix 8. This incident log must be monitored termly by the Principal/Head of Academy or designated SLT member.

12.9.2 Deliberate access to inappropriate materials by any user will lead to the incident being logged by the Online Safety Co-ordinator. Depending on the seriousness of the offence further action taken may include:

12.9.2.1 investigation by the Principal/Head of Academy/HR;

12.9.2.2 immediate sanctions, possibly leading to exclusion; or

12.9.2.3 involvement of police for very serious offences.

12.9.3 Users are made aware of sanctions relating to the misuse or misconduct through inductions and ongoing training (staff) and Computing lessons (students).

13. ANTI-VIRUS

All Delta PCs must have Delta's standard, supported anti-virus software installed and scheduled to run at regular intervals. In addition, the anti-virus software and the virus pattern files must be kept up-to-date. Virus-infected computers must be removed from the network until they are verified as virus-free. Academy Technical Leads are responsible for creating procedures that ensure anti-virus software is run at regular intervals, and computers are verified as virus-free. Any activities with the intention to create and/or distribute malicious programs into Delta's networks (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.) are prohibited. Failure to ensure devices are regularly updated may result in them becoming non-compliant and they will therefore be disabled until this is remediated.

14. PHISHING

14.1 Phishing emails are continuously being circulated and under no circumstances should users click on/open links if they appear to be suspicious. CITS can help both to identify and deal with these types of emails. CITS should always be contacted in the first instance when an email looks suspicious.

14.2 There are a few tips to help users identify possible phishing emails as follows:

- The domain name is spelt incorrectly or does not appear to be genuine.
- The email starts with an unfamiliar greeting or salutation (e.g. Dear customer, Dear member).
- The email has poor spelling and grammar.
- The email creates a sense of urgency.

15. COMPUTER USE

15.1 Appropriate measures must be taken when using computers to ensure the confidentiality, integrity and availability of sensitive information and that access to sensitive information is restricted to authorised users.

15.2 Staff and students using computers must consider the sensitivity of the information that may be accessed and minimise the possibility of unauthorised access.

15.3 Appropriate measures include:

15.3.1 restricting physical access to computers to only authorised people;

15.3.2 securing computers (screen lock or logout) prior to leaving an area to prevent unauthorised access;

15.3.3 enabling a password-protected screen saver with a short timeout period to ensure that computers that were left unsecured will be protected;

15.3.4 ensuring computers are used for authorised Trust purposes only;

15.3.5 never installing unauthorised software on computers; and

15.3.6 ensuring that monitors are positioned away from public view. If necessary, privacy screen filters or other physical barriers to public viewing will be installed.

16. CLEAR SCREEN

16.1 All users are expected to log off from their PCs/laptops when left for long periods and overnight.

16.2 When leaving their desk for lunch or to attend a meeting, users should lock down their screen using Ctrl, Alt, Del and then selecting Lock Workstation or Windows key and 'L'. Delta systems will do this automatically after 15 minutes; however, taking this measure will further reduce any security risk. NOTE: Academies may need longer than 15 minutes to cover timeout during lessons. This should be discussed and agreed with CITS before implementation.

16.3 Mobile devices through which access to the network can be obtained should be PIN protected, set to power off after a period of within 5 minutes and switched off when left unattended. These devices should be stored securely when not in use. (Exception: Tablets are not pin protected for ease of use).

17. COMPLAINTS

Complaints relating to online safety should be made to the Online Safety Co-ordinator or Principal/Head of Academy. Online safety incidents should be recorded using the log in **Appendix 8.**

18. REVIEW

This policy will be reviewed every three years, or when there are changes to relevant legislation or DfE guidance.

APPENDIX 1 – ACCEPTABLE USE AGREEMENT: DELTA STAFF, MEMBERS, TRUSTEES, AAB MEMBERS AND VISITORS

ICT and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in Delta and its Academies. All staff are expected to sign this agreement and adhere at all times to its contents. Any concerns or clarification should be discussed with the Academy online safety coordinator.

1. I will only use the Academy's email/Internet/Intranet/Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Principal/Head of Academy.

2. I will comply with the ICT system security and not disclose any passwords provided to me by the Academy or other related authorities.

3. I will ensure that all electronic communications with students and staff are compatible with my professional role.

4. I will not give out my own personal details, such as mobile phone number and personal email address, to students.

5. I will only use the approved, secure email system(s) for any Academy business.

6. I will ensure that personal data (such as data held on the Management Information System (MIS) and Office365) is kept secure and is used appropriately, whether in Academy, taken off the Academy premises or accessed remotely. Personal data can only be taken out of Academy or accessed remotely when authorised by the Principal/Head of Academy.

7. I will not install any hardware of software without permission of the ICT technician.

8. I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.

9. Images of students and/or staff will only be taken, stored and used for professional purposes in line with Academy policy and with the written consent of the parent, carer or staff member. Images will not be distributed outside the Academy network/ Office365 environment without the permission of the parent/carer, member of staff or Principal/Head of Academy.

10. I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Principal/Head of Academy.

11. I will respect copyright and intellectual property rights.

12. I will ensure that my online activity, both in Academy and outside Academy, will not bring my professional role into disrepute.

13. I will support and promote the Academy's online safety policy and help students to be safe and responsible in their use of ICT and related technologies.

User Signature

I agree to follow this Code of Conduct and to support the safe use of ICT throughout the Academy.

Signature:……..……Date…….

Full Name: ……..... (printed)

Job title: ……..

APPENDIX 2 - ACCEPTABLE USE AGREEMENT: STUDENTS

This agreement sets out the terms and conditions of use for students in the accessing ICT systems and Devices belonging to Delta Academies Trust (Trust) and/or the Academy. This agreement will apply to access of systems both within the academy and when accessing remote learning.

Remote learning may be accessed from a personal device or an academy loaned device. This agreement sets out the Trust's expectations in the use of its ICT systems and its loaned devices and ensures compliance with the Trust Online Safety Policy.

Specific to Remote Learning

Academy staff will initiate remote learning, with a timetable being shared with the Student/Parent/Carer in advance of the online learning.

Acceptable Use of IT within an Academy and for Remote Learning

1. Academy ICT software and systems, including the internet, email, digital video, mobile technologies, etc. will only be used for educational purposes.

2. Trust/Academy devices, including being used remotely, should be prioritised for educational purposes.

3. It is not permitted to download or install software on to an Academy device.

4. Log on to the Academy network/ Learning Platform will only be with the Student's own user name and password.

5. The Academy's ICT security system must be followed at all times and passwords should not be revealed or shared with anyone.

6. Student's Academy email address must be used while at the Academy or while using the Academy's equipment for accessing remote learning.

7. ICT communications with students, teachers or others, must be responsible and sensible.

8. Students will be responsible for their behaviour when accessing remote learning. Any abuse of the online platform, such as recording or capturing of images of staff, use of abusive language or interrupting a session with the streaming of inappropriate music or video imagery, will be followed up, with appropriate actions being taken.

9. Material that could be considered offensive or illegal must not be deliberately browsed, downloaded, uploaded or forwarded. Accidental access must be reported to a teacher immediately.

10. Sharing of a Student's personal information such as name, phone number or address is not allowed and they must not arrange to meet someone unless this is part of an Academy project approved by a teacher.

11. Images of students and/ or staff will only be taken, stored and used for Academy purposes in line with Academy policy and not be distributed outside the Academy network without the permission of the Principal/Head of Academy.

12. Online activity, both in Academy and outside Academy, will not cause the Academy, the staff, students or others distress or bring them into disrepute.

13. The privacy and ownership of others' work on-line at all times must be respected.

14. No attempt should be made to bypass the internet filtering system within an Academy or on a Trust or Academy device. Any issues with filtering then the academy should be contacted immediately.

15. The use of the Internet, Delta systems and the device within an academy or a device used remotely can be monitored and logged and information can be made available to teachers.

16. These rules are designed to keep Staff and Students safe, if not followed, Academy sanctions will be applied, and parent / carers or the Police may be contacted. Any safeguarding concerns will be raised with the academy Designated Safeguarding Lead (DSL).

Student Name

Full Name: …… (printed) Year:……..

Student Signature (Secondary only)

Signature:……Date: …….

Signed by the Parent/Carer (Required for Secondary and Primary)

Signature:……Date: …….

Note: By signing this agreement, you have agreed to follow the ICT Acceptable Use Agreement relating to the access of Academy ICT systems and devices whether within the Academy or remotely and that you agree to support the safe use of ICT in line with the Trust Online Safety Policy.

APPENDIX 2B – TRUST OR ACADEMY LOANED DEVICE

In certain circumstances, Delta Academies Trust (Trust) may decide that a loan device is required for a student to access remote learning.

1. Devices loaned by Delta Academies Trust must be used only in line with the Trust ICT acceptable use agreement.
2. The Parent/Carer will be responsible for ensuring the appropriate use of the device by their child. Filtering is provided on a Trust device; however, Parents/Carers should still ensure that their child is only accessing appropriate content.
3. If circumstances change and you are no longer in need of the loaned device, the device and accessories must be returned to the Academy immediately.
4. Loaned devices are the responsibility of the student/parent/carer and the Trust has an expectation that the device will be returned in the same condition as it was issued.
5. Any damage, loss or issues with a Trust device must be reported to the Academy immediately. Persistent abuse of devices and systems could lead to the removal of the device.
6. If devices are not used appropriately for the access of remote learning then the Trust reserves the right to recall the device.
7. The Trust reserves the right to recall a device at any time if deemed necessary.

Note: The Trust reserve the right to charge for any damage or non-return in line with Trust Charging Policy. Any charges will not exceed total replacement/repair costs.

Parent Signature

I agree to follow the above when loaning a device from Delta Academies Trust and understand my responsibilities.

Signature:…… Date:……..

Full Name:…… (printed)

APPENDIX 3 – PASSWORD CHARACTERISTICS AND GUIDELINES

1. Password Characteristics and Guidelines

1.1 Passwords must be composed of the following characteristics:

1.1.1 The password is at least **eight (8)** alphanumeric characters long for non-critical and non-admin accounts.

1.1.2 Critical Systems/user password should not be less than **fifteen (15)** alphanumeric characters (e.g. Built-in Admins, domain admins, and service accounts) whenever possible.

1.1.3 The password must contain both upper and lower case characters (e.g., a-z, A-Z). (This applies to staff only, students require any 8 characters).

1.2 The password must contain at least one numeric digit (e.g. 0-9) (This applies to staff only, students require any 8 characters). Passwords **should NOT** have the following characteristics:

1.2.1 A word found in a dictionary or a word in any language, slang, dialect, jargons etc.

1.2.2 Passwords shall not be the same as the username, login id, or Payroll number.

1.2.3 Default or generic passwords should not be used.

1.2.4 Passwords with common usage words such as: Password, Letmein etc.

1.2.5 Common names, family, pets, friends, co-workers, celebrities, famous historical figures…etc.

1.2.6 Computer terms and names, commands, sites, companies, hardware, software.

1.2.7 Personal information, addresses, birthdays, email, phone number etc.

1.2.8 Patterns such as abcdef, ASDFGH, zyxwvuts, 123321, 123456, 98765 etc.

1.2.9 Any of the above spelled backwards.

1.2.10 Any of the above preceded or followed by a digit (e.g. secret1, 1secret)

1.3 Creating memorable passwords:

One way to do this is by creating a password based on a song title, poems, affirmation, or other common phrase. (e.g., the phrase might be: "This May Be One Way to Remember" and the password could be "TmB1w2R!" or "Tmb1W>r~" or some other variation.

2. User Account Lockout

2.1 User accounts may be locked out as a result of unusual or suspicious behaviour. We proactively monitor access to user accounts.

2.2 For certain secured applications passwords may be changed when user access accounts are locked out more than **one (1)** time per **thirty-six (36)** hour period.

3. Password Reset

3.1 A user requiring a password reset for access to the standard Delta desktop must contact the CITS (Core IT Services) and provide sufficient detail to assure the service desk that their request is genuine.

3.2 A user requiring a password reset for access to a secured system must contact the CITS Service Desk, which may request further authorisation from the user department or system administration team dependant on the security policy for that particular application.

3.3 When the user uses the password provided by the ICT Service Desk they **MUST** change the password immediately at the next login.

4. Password History

4.1 Users may not re-use passwords they have previously used when their password expires. The password history will be the minimum of **eight (8)** passwords when possible.

4.2 If the CITS Service Desk needs user/desktop access so that they can gain physical access for work such as application installation or reimaging they will reset the password to a temporary one. Once the Service Desk team have completed their investigations they will inform the user of the temporary password which will have been set to expire at next login. The user should use the temporary password and change it immediately at the next login.

5. Application Developers

5.1 Application developers must **NOT** disclose their application development standards.

5.2 Application developers must ensure their programs contain the following security precautions:

5.2.1 Support authentication of individual users, not groups.

5.2.2 Do not store passwords in clear text or in any easily reversible form.

5.2.3 Provide for role based management to prevent privilege escalations.

6. Authentication Mechanisms

6.1 Information systems will authenticate all users. Passwords will be used as a base level of authentication.

6.2 Functions with high privilege and risk require strong multi-factor authentication, involving a password as well as one or more different authentication factors. Authentication options include hardware tokens, smartcards, alternative channels e.g. Public Key Infrastructure, (PKI), Certificates, Short Message Service (SMS), or callback, one-time passwords and biometrics.

6.3 Delta considers its cloud-based platform as a critical business system for communication and sharing information. As such, all staff accounts accessing Office365 from outside the Delta network will be subject to additional Multi Factor Authentication (MFA). Any issues arising from this must be passed to CITS for consideration.

7. Password Entry (Network Security)

7.1 Information systems must not retain account or password information from previous logins.

7.2 Passwords **must not** be shown as plain-text when they are entered by a user. A common masking symbol (e.g. asterisk) shall be displayed for every typed character.

7.3 All production system-level passwords **must** be part of the administered global password management system.

7.4 User accounts that have system-level privileges granted through group memberships or programs such as "sudo" **must** have a unique password from all other accounts held by that user.

8. Single Sign On (SSO)

Single Sign On (SSO) provides the mechanism of accessing multiple systems with one access. However, secure systems, or systems with higher IL level data should always require a separate authentication, and must not be accessed via SSO.

APPENDIX 4 – UNACCEPTABLE USE

Under no circumstances is an employee of Delta authorised to engage in any activity that is illegal under UK or international law while utilising Delta owned resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

1. System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1.1 Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Delta.

1.2 Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Delta or the end user does not have an active license.

1.3 Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.

1.4 Introduction of malicious programs into the network or server (e.g. viruses, worms, Trojan horses, e-mail bombs, etc.).

1.5 Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.

1.6 Using a Delta computing asset to engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws.

1.7 Making fraudulent offers of products, items, or services originating from any Delta account.

1.8 Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are

within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

1.9 Port scanning or security scanning is expressly prohibited unless prior notification to Delta is made.

1.10 Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.

1.11 Circumventing user authentication or security of any host, network or account.

1.12 Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).

1.13 Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.

1.14 Providing information about, or lists of, Delta's staff to outside parties.

2. Email and Communications Activities

The following activities are strictly prohibited, with no exceptions:

2.1 Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).

2.2 Any form of harassment via email or telephone whether through language, frequency, or size of messages.

2.3 Unauthorised use, or forging, of email header information.

2.4 Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.

2.5 Use of unsolicited email originating from within Delta's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by Delta or connected via the Delta network.

2.6 Posting the same or similar non-Trust-related messages to large numbers of users.

Staff may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production

services). Any exemption must be approved by your Line Manager before it is used.

2.7 The automatic forwarding of Delta Trust emails to email addresses or account outside the Trust.

APPENDIX 5 – MANAGING THE INTERNET SAFELY GUIDANCE

1. Internet Use Filtering System

1.1 CITS will block access to Internet websites and protocols that are deemed inappropriate for Delta's environment. The following protocols and categories of websites will be blocked:

1.1.1 Adult/Sexually Explicit Material;

1.1.2 Advertisements & Pop-Ups;

1.1.3 Chat and Instant Messaging;

1.1.4 Gambling;

1.1.5 Hacking;

1.1.6 Illegal Drugs;

1.1.7 Intimate Apparel and Swimwear;

1.1.8 Peer to Peer File Sharing;

1.1.9 Personals and Dating;

1.1.10 Social Network Services;

1.1.11 SPAM, Phishing and Fraud;

1.1.12 Spyware;

1.1.13 Tasteless and Offensive Content;

1.1.14 Violence, Intolerance and Hate; and

1.1.15 Certain, non-approved, Web Based Email.

2. Internet Use Filtering Rule Changes

The CITS will periodically review and recommend changes to web and protocol filtering rules. Changes to web and protocol filtering rules will be recorded in CITS protocols and will be available on request to staff of Delta.

3. Internet Use Filtering Exceptions

3.1 If a site is mis-categorised, staff may request the site be un-blocked by submitting a change request to CITS. CITS will review the request and un-block the site if it is mis-categorised.

3.2 Staff may access blocked sites with permission if access is appropriate and necessary for Trust purposes. If an employee needs access to a site that is blocked and appropriately categorised, they must submit a request (via the ICT servicedesk) to their Academy Principal/Head of Academy/Line Manager for approval which is then actioned by CITS.

4. Students

4.1 All students are advised to be cautious about the information given by others on sites, for example users not being who they say they are.

4.2 Students should avoid placing images of themselves (or details within images that could give background details) on such sites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online.

4.3 Students are always reminded to avoid giving out personal details on such sites which may identify them or where they are (full name, address, mobile/home phone numbers, academy details, IM/email address, specific hobbies/interests).

4.4 Students are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.

4.5 Students are encouraged to be wary about publishing specific and detailed private thoughts online.

4.6 Our students are asked to report any incidents of bullying to a member of staff at the Academy.

5. Staff

5.1 Staff may only create blogs, wikis or other online groups in order to communicate with students using the Microsoft Office 365 Cloud Platform or other systems approved by the Principal/Head of Academy.

5.2 Instances of Delta or the Academy being brought into disrepute may constitute misconduct or gross misconduct and disciplinary action will be taken. Staff should make clear whether they are communicating on behalf or the Academy or where opinions are their own.

5.3 An employee must not disclose confidential information relating to their employment at the Delta.

5.4 Sites must not be used to verbally abuse staff or students. Privacy and feelings of others should be respected at all times. Staff should obtain the permission of

individuals before posting contact details or pictures. Care should be taken to avoid using language which could be deemed as offensive to others.

5.5 If information on the site raises a cause for concern with regard to any conflict of interest, staff should raise the issue with their Line Manager.

5.6 If approached by a media contact about content on a site relating to Delta, staff should advise their line manager before taking any action.

5.7 Viewing and updating personal sites must not take place during working time unless agreed in advance as appropriate by your Line Manager. Access to Facebook is not permitted through any internet connection managed by Delta CITS (Core Information Technology Services) unless authorisation is obtained from CITS or your Line Manager.

5.8 Sites must not be used for accessing or sharing illegal content. Blogging from Delta's systems is subject to monitoring.

APPENDIX 6 – MICROSOFT TEAMS AND VIDEO CONFERENCING

1. Microsoft Teams and Video Conferencing - Guidance

1.1 Pupils/students could be asked to engage in online learning through the Microsoft 365 Platform (Teams) in the case or school closures or if there if an enhanced package of learning support available or allocated.

1.2 Permissions will be sought for activities outside of the normal routines of the academy.

1.2.1 Permission is sought from parents and carers if their children are involved in video conferences.

1.2.2 Permission is sought from parents and carers if their children are involved in video conferences with end-points outside of the Academy.

1.3 All pupils/ students are supervised by a member of staff when video conferencing.

1.4 All pupils/ students are supervised by a member of staff when video conferencing with end-points beyond the Academy.

1.5 In Secondary, students should only use the Microsoft 365 Platform, in particular the Teams App and use the Delta email address to access video conferencing. The Academy keeps a record of video conferences, including date, time and participants.

1.6 Approval from the Principal/Head of Academy is sought prior to all video conferences within Academy.

1.7 The Academy conferencing equipment is not set to auto-answer and is only switched on for scheduled and approved conferences.

1.8 No part of any video conference is recorded in any medium without the written consent of those taking part.

2. Additional points to consider

2.1 Participants in conferences offered by 3rd party organisations may not be DBS checked.

2.2 Conference supervisors need to be familiar with how to use the video conferencing equipment, particularly how to end a call if at any point any person taking part becomes unhappy with the content of the conference.

APPENDIX 7 – MOBILE TECHNOLOGIES GUIDANCE

1. Laptops

In order to minimise the potential risks, users must apply the following security controls:

1.1 The physical security of laptops is the personal responsibility of users who must take all reasonable precautions and be sensible and stay alert to the risks.

1.2 Users **must** keep laptops within their possession within sight whenever possible. They should never be left unattended in public view. Extra care should be taken in public places such as airports, railway stations or restaurants.

1.3 Where possible, laptops should be locked out of sight and must never be left unattended in a vehicle in public view. If absolutely necessary, it should be locked out of sight in the boot but it is generally safer for the user to take it with them.

1.4 Laptops should be carried and stored in a padded laptop computer bag or strong briefcase to reduce the chance of accidental damage. An ordinary-looking briefcase is also less likely to attract thieves than an obvious laptop bag.

1.5 In the event of loss or theft the Police must be notified immediately and Delta Core IT Service Desk informed as soon as practicable.

1.6 Information should not be stored on local hard drives unless there is no alternative.

1.7 Data encryption may be applied to all laptop hard drives owned by Delta.

2. Tablets, mobile phones and USB Sticks

2.1 These remain the property of Delta. In order to minimise any potential risks, users must apply the following security controls:

2.1.1 USB sticks should not be used and data should always be saved to the OneDrive cloud facility in the Microsoft 365 Platform.

2.1.2 Personal devices **must not** be connected to a laptop or desktop for any other purpose than re-charging the device.

2.1.3 No protectively marked information may be stored on a Mobile device unless it is encrypted and the device is locked with a PIN code.

2.1.4 It is the user's responsibility to ensure that sensitive information, is not be held on a mobile device for longer than is necessary. Sensitive information should not be included within the body of an email.

2.1.5 All spam, chain and other junk emails are subject to Delta's email policy.

2.1.6 The downloading of unauthorised software on to a Delta Device is prohibited.

2.1.7 Staff **must** report any suspected virus to the Delta Core ICT Service desk immediately and students should report this to their Learning Manager/relevant member of SLT/Line Manager.

2.2 Staff and students must take all appropriate steps to protect the mobile device from loss, theft or damage. These steps include, but are not limited to:

2.2.1 The mobile device **must not** be left unattended in public view in a vehicle,

2.2.2 The mobile device **must not** be left unattended in a public place.

2.2.3 The keypad **must** be locked at all times when the mobile device is not in use.

2.2.4 It is recommended that mobile devices are password/pin protected.

2.2.5 Users should be aware that Delta may deploy software to monitor the use of removable media devices and the transfer of information to and from all removable media devices and Delta owned IT equipment. It may prohibit the use of devices that have not been recorded on the Delta IT Asset Register. Management reports may be generated and used to support internal and external audit.

2.2.6 Damaged, faulty or infected devices must not be used.

2.2.7 Up-to date virus and malware checking software must be operational on both the machine from which the information is taken and the machine on to which the data is to be loaded. In order to implement this, it is necessary to regularly plug laptops into the Delta network.

APPENDIX 8 – ONLINE SAFETY INCIDENT LOG

Details of all online safety incidents to be recorded by the Online Safety Co-ordinator. This incident log will be monitored termly by the Principal/Head of Academy or designated member of the SLT.

Date and Time	Name of Student or Staff Member	Male or Female	Room and Computer/ Device Number	Details of Incident (including evidence)	Actions and Reasons