SUSSEX
LEARNING TRUST

Digital Safety & Wellbeing Policy

Version: 2.0

Approved by: Board of Trustees Date: 17/7/24

Custodian: D. Thomas

Terms: For ‘Headteacher’ read Executive Headteacher or Head of Academy

(1) Scope of the Policy

This policy applies to all members of the Trust’s community (including staff, students, volunteers, parents/ carers, visitors etc.) who have access to and are users of academy ICT systems, both in and out of academy.

The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students when they are off the academy site and empowers members of staff to implement the disciplinary policy for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other Digital Safety incidents covered by this policy.

The Trust will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate Digital Safety behaviour that take place out of academy.

(2) Roles and Responsibilities

The following section outlines the roles and responsibilities for Digital Safety of individuals and groups within the academy:

(2.1) Headteacher and Senior Leaders:

- The Headteacher is responsible for ensuring the safety (including Digital Safety) of members of the academy community, though they may delegate the day to day responsibility for Digital safety to another leader or Digital Safety Coordinator & wellbeing coordinator.

- The Headteacher/Senior Leaders are responsible for ensuring that the Digital Safety Coordinator and other relevant staff receive suitable CPD to enable them to carry out their Digital Safety roles and to train other colleagues, as relevant.

- The Headteacher/Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in the academy who carry out the internal Digital safety monitoring role. This is to provide a safety net and also support those colleagues who take on important monitoring roles.

- The Senior Leadership Team will receive regular monitoring reports from the Digital Safety Coordinator.

- The Headteacher and another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious Digital safety allegation being made against a member of staff.

(2.2) Digital Safety & Wellbeing Coordinator (academy specific)

- Takes day to day responsibility for Digital Safety issues and has a leading role in establishing and reviewing the academy Digital Safety policies.
- Ensures that all staff are aware of the procedures that need to be followed in the event of a Digital Safety incident taking place.
- Provides training and advice for staff.
- Liaises with the Local Authority.
- Liaises with Trust's Digital Services Team staff.
- Receives reports of Digital safety incidents and creates a log of incidents to inform future Digital safety developments
- Reports regularly to Senior Leadership Team

(2.3) Director of Digital Services & Network Team:

- Ensure that the Trustwide and individual academy's ICT infrastructure is secure and is not open to misuse or malicious attack.
- Ensure that the Trust's infrastructure meets the Digital Safety technical requirements outlined in national Digital Safety Policy and guidance.
- Ensure that users only access the academy's networks through properly enforced password protection guidelines (see appendix below), in which passwords are regularly changed.
- Keep up to date with Digital Safety technical information in order to effectively carry out their Digital Safety role and to inform and update others as relevant.
- Make sure that the use of the *network, Virtual Learning Environment (VLE), remote access, email* is regularly monitored in order that any misuse or attempted misuse can be reported to the *Digital Safety Coordinator for investigation, action and any associated sanctions.*

(2.4) All Trust staff:

- Ensure they have an up-to-date awareness of Digital Safety matters and of the current academy Digital Safety policy and practices.
- Ensure they have read and understood the academy Acceptable Use Agreement (AUA).
- Make sure they report any suspected misuse or problem to the Digital Safety & well-being Coordinator for investigation and action.
- Ensure that digital communications with students (email / Virtual Learning Environment (VLE) / voice) should be on a professional level and only carried out using official academy systems.
- Ensure that they are not 'friends' with students on social-networking sites and take every reasonable precaution to ensure that students cannot access personal content posted by them online.
- Ensure that Digital Safety issues are embedded in all aspects of the curriculum and other academy activities.

- Ensure that students understand and follow the academy Digital Safety and Acceptable User Agreement.

- Monitor ICT activity in lessons, extra-curricular and extended academy activities.

- Are aware of Digital Safety issues related to the use of mobile phones, tablet computers, cameras and other hand-held devices and that they monitor their use and implement current academy policies with regard to these devices.

(2.5) Designated Safeguarding Lead (for each academy):

- Should be trained in Digital Safety issues and be aware of the potential for serious child protection issues to arise from:

  - Sharing personal data
  - Access to illegal or inappropriate materials
  - Inappropriate on-line contact with adults (both known and unknown)
  - Incidents of grooming
  - Potential or actual
  - Cyber-bullying

(2.6) Students/pupils will be taught (see section 3 below) in a phase-differentiated manner :

- that they are responsible for using the academy ICT systems in accordance with the Student Acceptable Use Agreement

- to have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.

- to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.

- to know and understand academy policies on the use of mobile phones, tablet computers, digital cameras and other hand-held devices. They should also know and understand academy policies on the taking and use of images and on cyber-bullying.

- to understand the importance of adopting good Digital Safety practice when using digital technologies out of academy and realise that the academy's Digital Safety Policy covers their actions out of academy, if related to their membership of the academy.

(2.7) Parents/Carers:

Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet and mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The academy will therefore take every opportunity to help parents understand these issues through parents' evenings, letters and the website.

Parents and carers will be responsible for:

- Endorsing the Student Acceptable Use Agreement (AUA) on entry to a trust academy.

- Accessing the academy website, VLE and online student records in accordance with the relevant academy Acceptable Use Policy.

- Understanding the importance of talking to their child about their online profiles regularly (your child should be happy to show you their online profiles) and taking all reasonable precautions to ensure that their child/children are using the ICT resources available to them at home safely.

- Reporting to the academy any incidents that they become aware of (relating to their child or another child) that have occurred during academy time so that they can be dealt with quickly.

- Liaising with the academy on incidents that arise outside of academy time and working in partnership to deal with these accordingly.

(3) Education of Students

Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students in Digital Safety is therefore an essential part of the academy's digital safety & wellbeing provision. Children and young people need the help and support of the academy to recognise and avoid Digital Safety risks and build their resilience.

Digital safety & Wellbeing education will be provided in the following ways:

- A planned digital safety programme should be provided as part of ICT, Learning for Life and other lessons and should be regularly revisited – this will cover both the use of ICT and new technologies in academy and outside academy.

- Key digital safety and wellbeing messages should be reinforced as part of a planned programme of assemblies and tutorial and pastoral activities.

- Students should be taught in all lessons to be critically aware of the materials and content they access online and be guided to validate the accuracy of information.

- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the Internet.

(3.1) Education of Parents/Carers

Many parents and carers have only a limited understanding of Digital Safety risks and issues, yet they play an essential role in the education of their children and in the monitoring and regulation of the children's on-line experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it.

The trust will therefore seek to provide information and awareness to parents and carers through:

- Letters and the academy website
- Parents evenings

(3.2) Education & Training of Staff

It is essential that all staff receive Digital Safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- Digital Safety training will be made available to staff. An audit of the Digital Safety training needs of all staff will be carried out regularly.

- All new staff should receive Digital Safety training as part of their induction programme, ensuring that they fully understand the academy Digital Safety policy and Acceptable Use Policies.

- This Digital Safety Policy and its updates will be presented to and discussed by staff in staff or team meetings and at INSET days.

- The Digital Safety Coordinator (or other nominated person) will provide advice, guidance and training as required to individuals as required.

(3.3) Training of Governors & Trustees

Governors and Trustees should take part in Digital Safety training and awareness sessions, with particular importance for those who are members of any sub-committee or group involved in ICT, Digital Safety, health and safety and/or child protection. This may be offered through participation in academy training or information sessions for staff or parents.

(4) Technical – infrastructure, equipment, filtering and monitoring

The academy, in liaison with the Digital Services team, will be responsible for ensuring that the academy infrastructure and network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. Chief Officers have a responsibility in ensuring that central systems are treated in the same manner. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their Digital Safety responsibilities:

- There will be regular reviews and audits of the safety and security of academy ICT systems.
- Servers, wireless systems and cabling must be securely located and physical access restricted.
- All users will have clearly defined access rights to academy ICT systems.
- All users will be provided with a username and password by the Digital Services Team who will keep an up to date record of users and their usernames. Users will be required to change their password periodically.
- Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- Digital Services staff regularly monitor and record the activity of users on the academy ICT systems and users are made aware of this in the Acceptable Use Agreement.
- An appropriate system is in place for users to report any actual or potential Digital Safety incident to the Digital Services.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand-held devices etc. from accidental or malicious attempts which might threaten the security of the academy systems and data.
- An agreed policy is in place for the provision of temporary access of “guests” (e.g. trainee teachers, visitors) onto the academy system.
- An agreed policy is in place regarding the downloading of executable files by users
- The academy infrastructure and individual workstations are protected by up to date virus software.

(5) Curriculum

- Digital Safety should be a focus in all areas of the curriculum and staff should reinforce Digital Safety messages in the use of ICT across the curriculum.

- Where students are allowed to freely search the internet and/or use tablet computers, staff should be vigilant in monitoring the content of the websites the young people visit and the applications they are using.

- Students should be taught in all lessons to be critically aware of the materials and content they access on-line and be guided to validate the accuracy of information.

(6) Use of digital and video images - Photographic, Video

- Staff are allowed to take digital or video images to support educational aims, but must follow academy policies concerning the sharing, distribution and publication of those images (including checking against the list of students the academy will maintain listing students prohibited from having their images taken and published). Those images should only be taken on academy equipment; the personal equipment of staff should not be used for such purposes.

- Care should be taken when taking digital or video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the academy into disrepute.

- Students must not take, use, share, publish or distribute images of others without their permission.

- Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images.

- Students’ full names will not be used anywhere on a website or blog, particularly in association with photographs.

(7) Data Protection

Personal data will be recorded, processed, transferred and made available according to General Data Protection Regulation (GDPR) which states that personal data must be:

- Processed fairly, lawfully and in a transparent manor
- Used for specified, explicit and legitimate purposes
- Used in a way that is adequate relevant and limited
- Accurate and kept up to date
- Kept no longer than is necessary
- Processed in a manner that ensures appropriate security of the data

Staff must ensure that they:

- At all times take care to ensure the safekeeping of personal data, minimising the risk of its loss or misuse.

- Use personal data only on secure password protected computers and other devices, ensuring that they are properly “logged-off” at the end of any session in which they are using personal data. Transmit data under secure encrypted email or, if internally, within the Academies trust Gsuite ecosystem.

(See Data Protection Policy and Security Procedures documents)

(8) Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the academy currently considers the benefit of using these technologies for education outweighs their risks and any disadvantages:

	Staff & other Adults			Students			
	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission
Communication Technologies							
Mobile phones may be brought to academy	x				x[1]not seen		
Use of mobile phones in lessons		x					x
Use of mobile phones in social time	x			x			
Taking photos on mobile phones/cameras		x					x
Use of other mobile devices e.g. tablets and gaming devices		x					x
Use of personal email addresses in academy or on academy devices		X emergencies only				X emergencies only	
Use of academy email for personal emails		X emergencies only		x			
Use of messaging apps			x	x			
Use of Social media			x	x			
Use of Blogs			x				x

When using communication technologies, the academy considers the following as good practice:

- The official academy email service may be regarded as safe and secure.
- Users need to be aware that email communications may be monitored.
- Users must immediately report, to their form tutor or Head of Year, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff and students or parents / carers (email, chat, VLE etc) must be professional in tone and content.
- Personal information should not be posted on the academy or Trust website and only official email addresses should be used to identify members of staff.

(9) Unsuitable / inappropriate activities

[1] Primary academies may operate a system where phones have to be given in to an adult for safekeeping and returned at the end of the day.

The Trust believes that the activities referred to in the following section would be inappropriate in an academy context and that users, as defined below, should not engage in these activities in academy or outside academy when using academy equipment or systems. (This list should not be treated as exhaustive or definitive; it is for guidance only). The academy policy restricts certain internet usage as follows:

	Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X
Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
pornography				X	
promotion of any kind of discrimination				X	
threatening behaviour, including promotion of physical violence or mental harm				X	
any other information which may be offensive to colleagues or breaches the integrity of the ethos of the academy or brings the academy into disrepute				X	
Using academy systems to run a private business				X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the academy / academy				X	
Infringing copyright				X	

	Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)				X	
Creating or propagating computer viruses or other harmful files				X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)				X	
On-line gaming (educational)		X			
On-line gaming (non educational)		X			
On-line gambling				X	
On-line shopping / commerce for Trust/academy matters only		X			
File sharing	X				
Use of social media		X			
Use of messaging apps		X			
Use of video broadcasting eg Youtube		X			

(10) Responding to incidents of misuse:

It is expected that all staff will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse:

If any apparent or actual misuse appears to involve illegal activity i.e.

- child sexual abuse images
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials

The Digital Safety Coordinator, Headteacher or Chief Estates & Development Officer (Oversees Digital Services) should be informed immediately so that they can respond immediately.

If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (as above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation.

It is more likely that the Trust will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that learning points will be shared with relevant staff. It is intended that incidents of misuse will be dealt with through normal behaviour and disciplinary procedures as follows:
(This list should not be treated as exhaustive or definitive; it is for guidance only).

Staff **Likely actions to be Considered within our Disciplinary Policy**

Incidents:	Refer to line manager	Refer to Headteacher Principal	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc	Warning	Suspension	Consider disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X	X	X	X	X	X
Inappropriate personal use of the internet / social media / personal email	X	X	X			X		X

Unauthorised downloading or uploading of files	X	X	X			X		X
Allowing others to access academy network by sharing username and passwords or attempting to access or accessing the academy network, using another person's account	X	X	X	X		X	X	X
Careless use of personal data eg holding or transferring data in an insecure manner	X	X	X			X		
Deliberate actions to breach data protection or network security rules	X	X	X			X	X	X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	X	X	X	X		X	X	X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	X	X	X		X	X	X
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils	X	X	X			X		X
Actions which could compromise the staff member's professional standing	X	X	X			X	X	X
Actions which could bring the academy / academy into disrepute or breach the integrity of the ethos of the academy / academy	X	X	X			X	X	X
Using proxy sites or other means to subvert the academy's / academy's filtering system	X	X	X		X	X	X	X
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X	X			X	X	X
Deliberately accessing or trying to access offensive or pornographic material	X	X	X			X	X	X
Breaching copyright or licensing regulations	X					X		
Continued infringements of the above, following previous warnings or sanctions	X	X	X			X	X	X

Students / Pupils **Actions / Sanctions**

Incidents:	Refer to class teacher / tutor	Refer to Head of Department / Head of Year / other	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering / security etc	Inform Parents/ Carers	Removal of network / internet access rights	Warning	Further sanction eg detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X	X	X	X	X		X
Unauthorised use of non-educational sites during lessons	X	X					X	X	
Unauthorised use of mobile phone / digital camera / other mobile device	X	X						X	
Unauthorised use of social media / messaging apps / personal email	X	X						X	
Unauthorised downloading or uploading of files	X	X			X			X	
Allowing others to access academy / academy network by sharing username and passwords	X	X			X	X		X	X
Attempting to access or accessing the academy / academy network, using another student's / pupil's account	X	X	X	X	X	X		X	X
Attempting to access or accessing the academy / academy network, using the account of a member of staff	X	X	X	X	X	X	X	X	X
Corrupting or destroying the data of other users	X	X				X		X	X

Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	X	X			X		X	X
Continued infringements of the above, following previous warnings or sanctions	X	X	X			X	X	X	X
Actions which could bring the academy into disrepute or breach the integrity of the ethos of the academy	X	X	X			X	X	X	X
Using proxy sites or other means to subvert the academy's / academy's filtering system	X	X			X	X		X	X
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X			X	X		X	X
Deliberately accessing or trying to access offensive or pornographic material	X	X	X		X	X	X	X	X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	X	X				X		X	X

Appendix

Password Guidelines

1. Staff, pupils, students, Governors, Trustees and volunteers (known collectively as ‘digital users’) must always keep their password private, must not share it with others and must not leave it where others can find it.
2. All digital users have their own unique username and private passwords to access Trust systems.
3. Some digital users (determined by the Digital Services team and the sensitivity of the access the user has to sensitive data) have the extra protection of two factor authentication set up on their Google account systems. This gives extra protection if their password were to be compromised.
4. Staff are encouraged to change passwords regularly and maybe directed to do so by the digital services team at any time.

Guidance

- Don’t reveal a password over the phone to ANYONE.
- Don’t reveal a password in an email message.
- Don’t talk about a password in front of others.
- Don’t hint at the format of a password (e.g., “my family name”).
- Don’t reveal a password on questionnaires or security forms.
- Don’t share a password with family members.
- Don’t reveal a password to co-workers while on vacation.
- Don’t write a password in an obvious place that is accessible to others.

Document Version Control

Date	Version	Comment	Ratified by	Reviewer
11.2.21	1	Addition of password guidelines as an appendix	JM	JM
24/3/20	1	New Policy. Includes provisions previously in E-safety Policy	Board of Trustees 01/04/20	D Thomas & J Morris
20/1/21	1.1	No substantive changes, formatting only and inclusion of Appendix setting out password guidelines	Board of Trustees discussed at Board meeting on 10/2/21 and approved 17/2/21	D Thomas & J Morris
10/2/22	1.2	Review with no substantive changes: only dates updated	Board of Trustees 09/03/22	D Thomas M Sears
6/6/24	2.0	Review with no substantive changes	Board of Trustees 17/7/24	D.Thomas