Inspiring All to Excellence

The Fierté Multi-Academy Trust

Internet Safety Policy

Glascote Academy | Violet Way Academy | Ankermoor Primary | Dosthill Primary | Edge Hill Academy | Heathfields Infant and | Anker Valley Primary | Our Pride, Our Joy

Document Control

Policy Title	Internet Safety Policy
Effective Date	Spring 2021
Review Date	Spring 2022
Policy Owner	ITM/DPO
Policy Approver	Trust Board

Version Control

Version	Date	Amended by	Comments
V1	Spring 2020	L. Webster	Issued
V2	Spring 2021	Ryan Byrne	Revised technical details across multiple sections.

Section	Changes Made
1.5	Equity Statement added
2.1	Reference to Covid 19 and remote learning
3.2	Revised description of Technical Manager's role
3.5	Revised for accuracy of Forum responsibilities
4.4	Revised point on induction to clarify responsibility
4.6	Revised for accuracy
5.0	Removed grid defining levels of access as this varies across sites based-upon local academy leadership's preference

Contents:

Appendices

1. Rationale

1.1 Fierté Multi-Academy Trust recognises the internet and other digital technologies provide a vast opportunity for children and young people to learn and for educators to support and enhance learning. The Trust's drive to bring in mobile learning opportunities allows our community to promote creativity, stimulate awareness and enhance learning in lots of ways using technology.

1.2 This policy aims to ensure that there:

- Is a consistent Trust approach to Internet Safety
- Are clear, robust and integrated reporting routines
- Is coverage across the curriculum for pupils to engage with
- Is sufficient infrastructure in place to support digital learning while keeping the community safe
- Is training and known procedures for all aspects of e-safety and ICT usage for all pupils, staff, parents, Trustees and Governors
- Is clear and transparent monitoring and evaluation of Internet Safety practice carried out by the IT Strategy Forum

1.3 As part of our commitment to learning and achievement, the Trust wants to ensure that technology is used to:

- Raise educational standards and promote pupil achievement
- Develop the curriculum and make learning relevant, current and purposeful
- Enable pupils to gain access to a wide span of knowledge in a way that ensures their safety and security
- Enhance and enrich their lives and understanding

1.4 The Trust is committed to ensuring that all pupils will be able to use existing, as well as up and coming, technologies safely. We are also committed to ensuring that all those who work with children and young people are educated as to the risks that exist so that they can take an active part in safeguarding children.

1.5 This policy has been equality impact assessed and we believe that it is in line with the Equality Act 2010 as it is fair, it does not prioritise or disadvantage any individual and it helps to promote equality across Fierté Multi- Academy Trust.

2.0 Introduction

2.1 ICT in the 21st Century is an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. With the challenges arising as a result of the Coronavirus pandemic, IT has continued to

play a vital role in providing our learners with access to education. Consequently, schools must build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

2.2 Information and Communications Technology (ICT) covers a wide range of resources including web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Apps
- Email, Instant Messaging and chat ROOMS.
- Social Media, including Twitter and Facebook
- Mobile/Smart phones with text, video and/or web functionality
- Other mobile devices including tablets and gaming devices
- Online games
- Virtual Learning Environments
- Blogs and Wikis
- Podcasting
- Video sharing
- Downloads
- On-demand TV and video, movies
- Smart TVs

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies and that some have minimum age requirements (in most cases this is 13 years old).

At Fierté Multi-Academy Trust, we understand the responsibility to educate our pupils on E-Safety Issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, both in and beyond the context of the classroom.

Academies hold personal data on learners, staff and others to help them conduct their day- to-day activities. Some of this information is sensitive and could be used by another person or criminal organisation to cause harm or distress to an individual. The loss of sensitive information can result in media coverage, and potentially damage the reputation of the Trust. This can make it more difficult for academies to use technology to benefit learners. Everybody in the Trust community has a shared responsibility to

secure any sensitive information used in their day to day professional duties and even staff not directly involved in data handling should be made aware of the risks and threats and how to minimise them.

Both this policy and the Acceptable Use Agreement (for all staff, trustees, governors, volunteers, and pupils) are inclusive of technologies provided by the Trust (such as PCs, laptops, tablets, mobile devices, webcams, whiteboards, cameras, digital video equipment, etc); and devices owned by pupils and staff, but brought onto academy premises (such as laptops, mobile phones and other mobile devices).

3.0 Internet Safety Roles and Responsibilities

3.1 As Internet Safety is an important aspect of strategic leadership within the Trust, the Head and Governors of each academy have ultimate responsibility to ensure that the policy and practices are embedded and monitored.

Each Academy has an IT Lead member of staff who has day to day responsibility of Internet Safety in each school. It is part of their role to ensure staff are aware of procedures that need to be followed in the event of an online safety incident taking place. They provide advice and training for staff to ensure Internet Safety is embedded in all aspects of the curriculum.

3.2 Although Fierté Multi-Academy Trust have entered into a number of IT-related service level agreements with external ICT service providers, it is the responsibility of the Trust to ensure the managed service provider (MSP) is fully aware of the Trust's Online Safety Policies and Procedures. As such, in some cases, representatives from key MSPs are invited to attend as members of the Trust IT Strategy Forum.

To co-ordinate the provision and management of IT services, in September 2019, the role of Trust Technical Manager was developed. The Technical Manager monitors IT services and works alongside academy IT Curriculum Leadersfrom across the Trust to ensure that the academies are supported in the safe use of technology. At present, strategiclevel responsibility for IT remains with the Trust Vice-CEO – to whom the Technical Manager reports directly.

3.3 All Teaching and Support Staff across the Trust are responsible for ensuring that:

- They have an up to date awareness of online safety matters and of the current school / academy Online Safety Policy and practices.
- They have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP).

- They immediately report any suspected misuse or problem to theTechnical Manager for investigation / action.
- All digital communications with staff / pupils / parents / carers are on a professional level and only carried out using official school systems.
- Online safety issues are embedded in all aspects of the curriculum and other activities.
- Staff / pupils understand and follow the Online Safety Policy and acceptable use policies.
- Staff / pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- The use of digital technologies, mobile devices, cameras etc. in lessons and other school activities (where allowed) is monitored and current policies related to the use of these devices are implemented.
- In lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

3.4 All designated safeguarding members of staff should be trained in Online Safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- online-bullying

Note: it is important to emphasise that these are safeguarding issues, not technical issues, the technology simply provides additional means for safeguarding issues to develop.

3.5 The IT Strategy Forum provides a consultative group that has wide representation from the Trust community, with responsibility for issues regarding online safety and the monitoring of the Internet Safety Policy including the impact of initiatives. The group are also responsible for regular reports to the Trust Board.

Members of the IT Strategy Forum will support IT Leads (or other relevant personnel, as above) with:

- The production / review / monitoring of the school Online Safety Policy / documents.
- Mapping and reviewing the online safety / digital literacy curricular provision – ensuring relevance, breadth and progression.

- Identifying developing technologies, solutions and systems which may be of value to academies.
- Consulting stakeholders – including parents / carers and the pupils about the online safety provision.

3.6 All pupils are responsible for using the academy digital technology systems in accordance with the Pupil Acceptable Use Agreement. They should also:

- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- Understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on online bullying.
- Understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the Trust's Internet Safety Policy covers their actions out of school, if related to their membership of the Trust.

3.7 Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The Trust will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about national / local online safety campaigns and literature. Parents and carers will be encouraged to support the Trust in promoting good online safety practice and to follow guidelines on the appropriate use of:

- Digital and video images taken at school events.
- Access to parents' sections of the website and on-line student records.

3.8 Governors / Trustees and Volunteers who access academy systems as part of the academy provision will be expected to sign an Acceptable User Agreement before being provided with access to school / academy systems.

4.0 Policy Statements

4.1 Education – Pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety / digital literacy is therefore an essential part of the Trusts internet safety provision. Children and young people need the help and support of our academies to recognise and avoid online safety risks and to build their resilience.

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The internet safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned online safety curriculum should be provided as part of Computing / PSHE / other lessons and should be regularly revisited.
- Key online safety messages should be reinforced as part of a planned programme of assemblies through learning and PSHE activities.
- Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Pupils should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.
- Pupils should be helped to understand the need for the Pupil Acceptable Use
- Agreement and encouraged to adopt safe and responsible use both within and outside the academy.
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices.

In lessons where internet use is pre-planned, it is best practice that pupils are guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites young people visit.

It is accepted that from time to time, for good educational reasons, pupils may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Trust Technical Manager (or other relevant designated person) temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need. In some circumstances, the Technical Manager may also require additional authorisation from the academy's SLT before proceeding.

4.2 Education – Parents / Carers

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of children's online behaviours. Parents may underestimate how

often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

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

- Curriculum activities
- Letters, newsletters, web site.
- Parents / Carers evenings / sessions
- High profile events / campaigns e.g. Safer Internet Day Reference to the relevant web sites / publications e.g..
  swgfl.org.uk saferinternet.org.uk
  childnet.com/parents-and-carers

4.3 Education – The Wider Community

The Trust may provide opportunities for local community groups / members of the community to gain from the academy's online safety knowledge and experience. This may be offered through the following:

- Providing family learning courses in use of new digital technologies, digital literacy and online safety.
- Online safety messages targeted towards grandparents and other relatives as well as parents.
- The Trust / academy website may provide online safety information for the wider community.
- Supporting community groups e.g. Early Years Settings, Childminders, youth / sports / voluntary groups to enhance their Online Safety provision. (possibly supporting the group in the use of Online Compass, an online safety self-review tool for groups such as these - onlinecompass.org.uk)

4.4 Education and Training – Staff / Volunteers

It is essential that all staff / volunteers receive online safety training and understand their responsibilities, as outlined in this policy. CPD will be offered as follows:

- A tailored programme of online safety training will be made available to staff. This will be regularly updated and reinforced. All staff will annually undertake an audit of internet safety training needs.
- All new staff / volunteers should receive online safety training from academies as part of their induction programme, ensuring that they fully understand the Trust Internet Safety Policy and Acceptable Use Agreements.
- It is expected that some staff will identify online safety as a training need within the performance management process.

- The IT Curriculum Lead will receive regular updates through attendance at external training events (e.g. from Becta, SWGfL / LA / other relevant organisations) and by reviewing guidance documents released by relevant organisations.
- This Internet Safety Policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.
- The IT Lead will provide advice / guidance / training to individuals as required.
- Guest users will be issued with an Abridged Internet Safety Policy also asked to sign an Acceptable Use Agreement as part of the Supply Staff pack.

4.5 Training – Governors / Trustees

Governors / Trustees should take part in online safety training / awareness sessions, with particular importance for those who are members of any academy involvement in technology / online safety / health and safety / safeguarding. This may be offered in a number of ways:

- Attendance at training provided by the MAT / National Governors Association / or other relevant organisation (e.g. SWGfL).
- Participation in Trust / academy training sessions for staff or parents (this may include attendance at assemblies / lessons).

4.6 Technical – infrastructure / equipment, filtering and monitoring

The Trust will be responsible for ensuring that our academies infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people in the above sections will be effective in carrying out their online safety responsibilities.

Trust / Academy technical systems will be managed in ways that ensure that the Trust / academy meets recommended technical requirements.

- There will be regular reviews and audits of the safety and security of academy technical systems. Suggested actions arising from these reviews will be shared with the Vice CEO in their role as Trust Strategic IT Leader.
- Sensitive network equipment must be securely located with physical access restricted. Where this is not the case, the Trust Technical Manager will raise the concern with academy leadership teams.
- All users will have clearly defined access rights to Trust / academy technical systems and devices.
- All users will be provided with a username and password by the Trust Technical Team. Users are responsible for the security of their username and password. An up-to-date record of users will be available from the Trust Technical Manager upon request.

Admin credentials for IT systems are stored centrally in encrypted password management software. Each member of the Trust Technical Team is granted access to shared folders within this software relevant to their roles.

Administrator passwords are not shared with members of staff except for in exceptional circumstances.

The Trust Technical Manager is ultimately responsible for ensuring that software licenses are accurate and up to date and that regular checks are made to reconcile the number of licenses purchased against the number of users/ installations.

In executing this responsibility, the Trust recognise that the Technical Manager will be reliant upon information provided by others.

Inadequate licensing could cause academies to breach the Copyright Act which could result in fines or unexpected licensing costs.

While onsite, DNS-based filtering is provided by a managed service provider for all users.

Content lists are regularly updated and internet usage is logged. Internet filtering / monitoring should ensure that children are safe from illegal and extremist material when accessing the internet. However, no technical solution can detect and restrict all such content and, consequently, academies should immediately report any sites which bypass these measures.

- Each academy system has provided enhanced / differentiated user-level filtering (allowing different filtering levels for different ages / stages and different groups of users – staff / pupils etc). Upon installation of new filtering systems, policies are agreed first with headteachers and/or academy leadership teams.
- Where possible, the activity of users on academy technical systems is logged and users are made aware of this in the Acceptable Use Agreement.
- Appropriate security measures are in place to protect the managed infrastructure and end-user devices from accidental or malicious attempts which might threaten the security of academy systems and data. Where the Trust Technical Manager identifies that any existing measures are not adequate, they will report to the Vice-CEO and identify suggested measures to remedy the situation. Where security and patch support for devices and equipment ends, the Trust Technical Manager will provide recommended next steps to the Vice-CEO and academy leadership teams.

- An agreed policy is in place (Supply Teacher Information Pack) for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto school systems.
- It is the responsibility of headteachers to notify the Trust Technical Team in advance (*minimum 2 working days*) of any users for which access must be terminated.
- An agreed policy is in place (Laptop/Tablet) regarding the extent of personal use that staff and their family members are allowed on academy devices that may be used out of school.
- An agreed policy is in place (Data Protection Policy) regarding the use of removable media (e.g. memory sticks / CDs / DVDs) by users on school devices.
- Personal data must not be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.
- The Trust accept that the Technical Manager and Technical Team can only manage compliance of systems and devices of which they have been appropriately consulted on and granted sufficient levels of access.

5.0 Mobile Technologies

Mobile technology devices may be academy owned/provided or personally owned and might include: smartphones, tablets, laptops or other technology that usually has the capability of utilising the academy's network. These devices may have access to the wider internet which may include academy and other cloud based services such as email and data storage.

All users should understand that the primary purpose of the use mobile / personal devices in a school context is educational. The mobile technologies policy should be consistent with and inter-related to other relevant school polices including but not limited to the Safeguarding Policy, Behaviour Policy, Anti-Bullying Policy, Acceptable Use Policy, and policies around theft or malicious damage. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the school's Online Safety education programme. The Acceptable Use Agreements for staff, pupils, parents / carers and volunteers / governors / trustees will give consideration to the use of mobile technologies.

6.0 Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to

individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular, they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the Trust / academy websites / social media / local press.
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at academy events for their own personal use. To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other pupils in the digital / video images.
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow academy policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school / academy equipment; the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school / academy into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Pupil's work can only be published with the permission of the pupil and parents or carers.

7.0 Data Protection

Personal data will be recorded, processed, transferred and made available according to the current GDPR data protection legislation, as stated in the Trust's Data Protection Policy. Staff must ensure that they:

At all times take care to ensure the safe keeping 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.
- Transfer data using encryption and secure password protected devices.

When personal data is stored on any portable computer system, memory stick or any other removable media:

- The data must be encrypted and password protected.
- The device must be password protected.
- The device must offer approved virus and malware checking software.
- The data must be securely deleted from the device, in line with Trust policy once it has been transferred or its use is complete.

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

Communication Technologies	Staff				Other Adults		Pupils
	Allowed	Not allowed	Allowed at certain times	Allowed for selected staff	Allowed at certain times	Not allowed	Not allowed
Mobile phones may be brought to the academy							
Use of mobile phones in lessons							
Use of mobile phones in social time							
Taking photos on personal mobile phones / cameras							
Use of other personal mobile devices e.g. tablets, gaming devices							
Use of personal email addresses in academy , or on academy network							
Use of academy email for personal emails							
Use of messaging apps							
Use of social media							
Use of blogs							

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

- The Trust email service may be regarded as secure and users should be aware that email and Teams communications are logged. Staff and pupils should therefore use only the academy email or messaging service to discuss school-related matters...
- Pupil's Office 365 accounts should have communication restricted (*with email and 1:1 Teams chat disabled*) with only specific exceptions being applied at the request of academy leaders.
- Users must immediately report, to the nominated person – in accordance with the

-

Trust policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.

Any digital communication between staff and pupils or parents / carers (email, social media, chat, blogs, VLE etc.) must be professional in tone and content. These communications may only take place on official (monitored) academy systems. Personal email addresses, text messaging or social media must not be used for these communications.

- Pupils will be provided with individual academy email addresses for educational use.
- Pupils should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the academy website and only official email addresses should be used to identify members of staff.

8.0 Social Media

8.1 Protecting Professional Identity

All schools, academies, MATs and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools/academies, MATs and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, engage in online bullying, discriminate on the grounds of sex, race or disability or who defame a third party may render the academy or MAT liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The Trust provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through:

- Ensuring that personal information is not published.
- Training is provided including: acceptable use; social media risks; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions.
- Risk assessment, including legal risk.

Trust / academy staff should ensure that:

- No reference should be made in social media to pupils, parents / carers or academy staff.
- They do not engage in online discussion on personal matters relating to members of the school community.
- Personal opinions should not be attributed to any academies in the Trust.

- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

When official academy social media accounts are established there should be:

- A process for approval by senior leaders.
- Clear processes for the administration and monitoring of these accounts – involving at least two members of staff.
- A code of behaviour for users of the accounts, including:
  - Systems for reporting and dealing with abuse and misuse.
  - Understanding of how incidents may be dealt with under academy disciplinary procedures.

Personal Use:

- Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the Trust / academy or impacts on the Trust / academy, it must be made clear that the member of staff is not communicating on behalf of the Trust / academy with an appropriate disclaimer. Such personal communications are within the scope of this policy.
- Personal communications which do not refer to or impact upon the school are outside the scope of this policy.
- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken.
- The Trust / academy permits reasonable and appropriate access to private social media sites.

Monitoring of Public Social Media

- As part of active social media engagement, it is considered good practice to proactively monitor the Internet for public postings about the Trust / academies.
- The Trust should effectively respond to social media comments made by others according to a defined policy or process.

The academy's use of social media for professional purposes will be checked regularly by the members of the IT Strategy Forum to ensure compliance with Trust policies.

9.0 Dealing with unsuitable / inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from academy and all other technical systems. Other activities e.g. cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but

would be inappropriate in an academy context, either because of the age of the users or the nature of those activities.

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 / or outside the academy when using academy equipment or systems. The Trust policy restricts usage as follows:

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	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	
	Promotion of extremism or terrorism				X	

	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the Trust or brings the Trust into disrepute				X	
Using school 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					X	
Infringing copyright					X	
Revealing or publicising confidential or proprietary information (e.g. 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	
Educational on-line games	X					
On-line gambling					X	
On-line shopping / commerce					X	
File sharing	X					
Use of social media		X				
Use of messaging apps		X				
Use of video broadcasting e.g. YouTube		X				

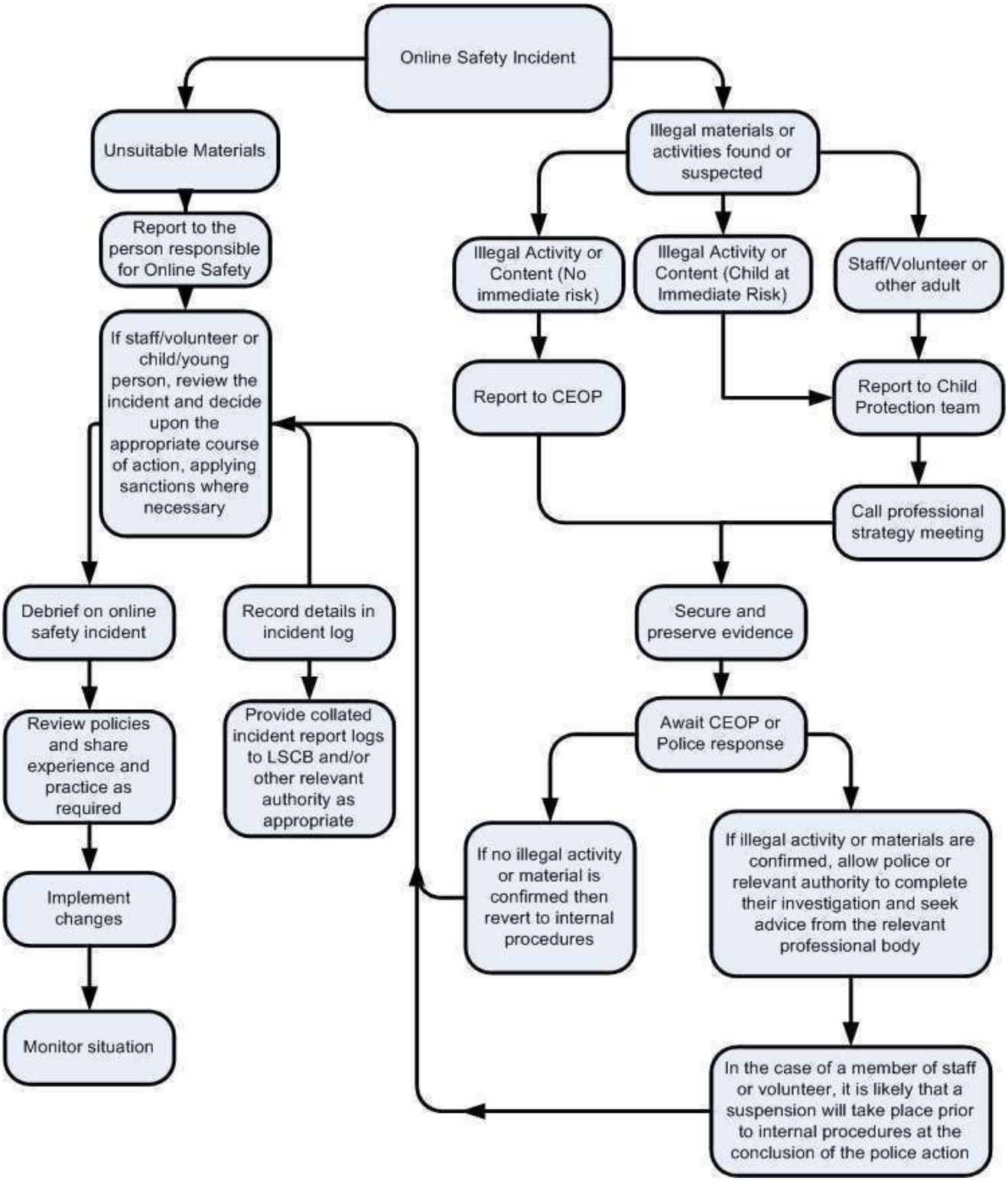
10. Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident.

Incidents might involve illegal or inappropriate activities (see "User Actions" above).

11. Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart for responding to online safety incidents and report immediately to the police.



12. Other Incidents

It is hoped that all members of the Trust community will be responsible users of digital technologies, who understand and follow the Trust policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below).
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
  - Internal response or discipline procedures o Involvement by Trust Board or national / local organisation (as relevant).
  - Police involvement and / or action.
- If content being reviewed includes images of child abuse, then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include: o Incidents of 'grooming' behavior. o The sending of obscene materials to a child. o Adult material which potentially breaches the Obscene Publications Act. o Criminally racist material. o Promotion of terrorism or extremism.
  - Other criminal conduct, activity or materials.
- Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for the Trust / academy and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

13. Cyberbullying

Cyberbullying is the use of ICT, particularly mobile phones and the internet, to deliberately upset someone else. The whole Trust community has a duty to protect all its members and provide a safe, healthy environment. The Educations and Inspections Act

2006 states that Headteachers have the power 'to such an extent as is reasonable' to regulate the conduct of pupils when they are off site. It is important that we work in partnership with pupils and parents/carers to educate them about Cyberbullying as part of internet safety.

They should:

- Understand how to use these technologies safely and know about the risks and consequences of misusing them.
- Know what to do if they or someone they know are being cyber bullied.
- Report any problems with Cyberbullying. If they do have a problem, they can talk to the academy, parents/carers, the police, the mobile network (for phone) or the Internet Service Provider (ISP) to do something about it.

14. Trust / Academy Actions and Sanctions

It is more likely that the Trust / academy 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 members of the Trust community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures as follows:

	Actions / Sanctions								
Pupil Incidents	Refers to class teacher	Refers to IT Lead	Refers to Headteacher/Principal	Refers to Police	Refers to technical support staff for action re: filtering / security etc.	Inform parents / carers	Removal of network / internet access	Warning	Further sanction eg: exclusion
Deliberately accessing or trying to access material that could be		X				X			

considered illegal (see list in earlier section on unsuitable / inappropriate activities).									
Unauthorised use of non-educational sites during lessons	X							X	
Unauthorised / inappropriate use of mobile phone / digital camera / other mobile device			X			X			
Unauthorised / inappropriate use of social media / messaging apps / persona email			X			X			
Unauthorised downloading or uploading of files	X								
Allowing others to access academy network by sharing username and passwords	X							X	
Attempting to access or accessing the academy network, using another pupil's account	X							X	
Attempting to access or accessing the academy network, using the account of a member of staff			X			X	X		
Corrupting or destroying the data of other users		X							
Sending an email, text or			X			X	X	X	X

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

	Actions / Sanctions

Staff Incidents	Refer to line manager	Refer to Headteacher/Principal	Refer to DPO	Refer to Executive Team	Refer to Police	Refer to Technical Support Staff for action re: filtering etc.	Warning	Suspension	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
Inappropriate personal use of the internet / social media / personal email		X					X		C
Unauthorised downloading or uploading of files.	X	X							
Allowing others to access Trust / academy network by sharing username and passwords or attempting to access or accessing the Trust / academy network, using another person's account	X	X	X			X			
Careless use of personal data e.g. holding or transferring		X	X			X			

data in an insecure manner									
Deliberate actions to breac data protection or network security rules		X	X			X			
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		X	X			X			
Sending an email, text or message that is regarded a offensive, harassment or of bullying nature		X					X		X
Using personal email / social networking / instant messaging / text messaging to carrying ou digital communications with pupils and parents		X							X
Actions which could compromise the staff member's professional standing		X					X		
Actions which could bring the Trust / academy into disrepute or breach the integrity of the ethos of the Trust		X							
Using proxy sites or other means to subvert the academy's filtering system		X		X			X		X
Accidentally accessing offensive or pornographic material and failing to report the incident		X				X			
Deliberately accessing or trying to access offensive o pornographic material		X		X	X	X	X		X
Breaching copyright o licensing regulations		X	X			X			

Continued infringements of the above, following previous warnings or sanctions		X		X	X				X

15. Monitoring and evaluation

The policy will be monitored and evaluated regularly taking into account any incidents which occur or technological developments which might need a change in the policy.

16. Links with other policies

This Internet Safety Policy is linked to our:

Data Protection Policy
Policy for the safe use of children's photographs
Safeguarding Policy
Behaviour Policy
Bring Your Own Device to Work (BYOD) Policy
Mobile Device and Camera Policy
Email Policy

Appendices

Pupil Acceptable Use Agreement – KS2
Pupil Acceptable Use Agreement – Early Years and KS2
Parent / Carer Acceptable Use Agreement
Staff Acceptable Use Agreement
Volunteer / Trustee / Governor Acceptable Use Agreement
Temporary User Acceptable Use Agreement
Reporting Log
Training Needs Log

Fierté Multi Academy Trust

Pupil Acceptable Use Agreement KS2

When I use the school's ICT facilities (like computers and equipment) and get on the internet in school, I will not:

- Use them without asking a teacher first, or without a teacher in the room with me
- Use them to break school rules
- Go on any inappropriate websites
- Go on Facebook or other social networking sites (unless my teacher said I could as part of a lesson)
- Use chat rooms
- Open any attachments in emails, or click any links in emails, without checking with a teacher first
- Use mean or rude language when talking to other people online or in emails
- Share my password with others or log in using someone else's name or password Bully other people

I understand that the school will check the websites I visit and how I use the school's computers and equipment. This is so that they can help keep me safe and make sure I'm following the rules. I will tell a teacher or a member of staff I know immediately if I find anything on a school computer or online that upsets me, or that I know is mean or wrong.

I will always be responsible when I use the school's ICT systems and internet.

I understand that the school can discipline me if I do certain unacceptable things online, even if I'm not in school when I do them.

Class: …….

Date: …….

Fierté Multi Academy Trust

Signed:

Pupil Acceptable Use Agreement Early Years and KS1

All internet and e-mail activity in our academy is monitored.

These Internet Safety Rules help to protect us and our academy by describing acceptable and unacceptable computer use.

Our Fierté Academy Rules

- I ask before I use the computer/ tablet.
- I only go on websites I'm allowed on.
- I never share my personal information.

If something makes me feel worried, then I tell an adult.

If I break these rules, I know something will happen.

Class: ……..

Date: ……..

Signed:

Fierté Multi Academy Trust

Parent / Carer Acceptable Use Agreement

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies provide powerful tools, which open up new opportunities for everyone. They can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- That young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- That academy systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- That parents and carers are aware of the importance of online safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

Our academies will try to ensure that pupils will have good access to digital technologies to enhance their learning and will, in return, expect the pupils to agree to be responsible users. A copy of the Pupil Acceptable Use Policy is attached to this permission form, so that parents / carers will be aware of the Trusts expectations of the young people in their care.

Parents are requested to sign the permission form below to show their support of the Trust in this important aspect of the Trust's work.

Permission Form

Parent / Carers Name: ……

Child's Name: …….

As the parent / carer of the above pupil, I give permission for my son / daughter to have access to the internet and to ICT systems at school.

I understand that the school has discussed the Acceptable Use Agreement with my son / daughter and that they have received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

I understand that the academy will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and systems. I also understand that the academy cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my son's / daughter's activity on the systems will be monitored and that the academy will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the Academy if I have concerns over my child's online safety.

Signed: …….

Date: …….

Fierté Multi Academy Trust

Staff Acceptable Use Agreement

New technologies have become integral to the lives of children and young people in today's society, both within schools / academies and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe access to the internet and digital technologies at all times.

This Acceptable Use Policy is intended to ensure:

- that staff will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that academy systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of technology in their everyday work.
- Our academies will try to ensure that staff will have good access to digital technology to enhance their work, to enhance learning opportunities for pupils learning and will, in return, expect staff to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that students / pupils receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

For my professional and personal safety:

- I understand that the academy will monitor my use of academy digital technology and communications systems.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email, VLE etc.) out of school, and to the transfer of personal data (digital or paper based) out of school.
- I understand that academy digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.

- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using academy ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the Trust policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the Trust / academy websites / Teams) it will not be possible to identify by name, or other personal information, those who are featured. I will only use social networking sites in school in accordance with the Trust's policies.
- I will only communicate with students / pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The Trust have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the academy:

- When I use my mobile devices (laptops / tablets / mobile phones / USB devices etc.) in school, I will follow the rules set out in this agreement, in the same way as if I was using academy equipment. I will also follow any additional rules set by the school / academy about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not use personal email addresses on the academy ICT systems.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programs).
- I will ensure that my data is regularly backed up, in accordance with relevant academy policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try

to use any programs or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.

- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programs of any type on a machine, or store programs on a computer, nor will I try to alter computer settings, unless this is allowed in school / academy policies.
- I will not disable or cause any damage to academy equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the Trust Data Protection Policy (or other relevant policy). Where digital
- personal data is transferred outside the secure local network, it must be encrypted. Paper based Protected and Restricted data must be held in lockable storage.
- I understand that data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by Trust policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for academy sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of the academy:

- I understand that this Acceptable Use Policy applies not only to my work and use academy digital technology equipment in school, but also applies to my use of academy systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the academy
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors / Executive Leadership Team and Trustees, and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use academy digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the Trust / academy) within these guidelines.

Staff Name: ……

Signed: ……

Date: ……

Fierté Multi Academy Trust

Volunteer / Trustee / Director / Governor Acceptable Use Agreement

New technologies have become integral to the lives of children and young people in today's society, both within schools / academies and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe access to the internet and digital technologies at all times.

This Acceptable Use Policy is intended to ensure:

- that volunteers / trustees / directors / governors will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that academy systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that volunteers / trustees / directors / governors are protected from potential risk in their use of technology in their everyday work.

Our academies will try to ensure that volunteers / trustees / directors /governors will have good access to digital technology to enhance their work, to enhance learning opportunities for pupils learning and will, in return, expect volunteers / trustees / directors /governors to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that students / pupils receive opportunities to gain from the use of digital technology. I will, where possible, educate

the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

For my professional and personal safety:

- I understand that the academy will monitor my use of academy digital technology and communications systems.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email, VLE etc.) out of school, and to the transfer of personal data (digital or paper based) out of school.
- I understand that academy digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school. (schools should amend this section in the
- light of their policies which relate to the personal use, by volunteers / trustees / directors / governors, of academy systems)
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using academy ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the Trust policy on the use of digital / video images.
- I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the Trust / academy websites / Teams) it will not be possible to identify by name, or other personal information, those who are featured. I will only use social networking sites in school in accordance with the Trust's policies.
- I will only communicate with students / pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The Trust have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the academy:

- When I use my mobile devices (laptops / tablets / mobile phones / USB devices etc.) in school, I will follow the rules set out in this agreement, in the same way as if I was using academy equipment. I will also follow any additional rules set by the school / academy about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not use personal email addresses on the academy ICT systems.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programs)
- I will ensure that my data is regularly backed up, in accordance with relevant academy policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to
- use any programs or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programs of any type on a machine, or store programs on a computer, nor will I try to alter computer settings, unless this is allowed in school / academy policies.
- I will not disable or cause any damage to academy equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the Trust Data Protection Policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based Protected and Restricted data must be held in lockable storage.
- I understand that data protection policy requires that any volunteers / trustees / directors / governors or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by Trust policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for academy sanctioned personal use:
I will ensure that I have permission to use the original work of others in my own work Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of the academy:

- I understand that this Acceptable Use Policy applies not only to my work and use academy digital technology equipment in school, but also applies to my use of academy systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the academy
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors / Executive Leadership Team and Trustees, and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use academy digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the Trust / academy) within these guidelines.

Volunteers / Trustees / Directors / Governors Name: …….

Signed: ……

Date: ……

Fierté Multi Academy Trust

Guest User Acceptable Use Agreement

New technologies have become integral to the lives of children and young people in today's society, both within schools / academies and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe access to the internet and digital technologies at all times.

This Acceptable Use Policy is intended to ensure:

- that guest users will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that academy systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- That guest users are protected from potential risk in their use of technology in their everyday work.

Our academies will try to ensure that guest users will have good access to digital technology to enhance their work, to enhance learning opportunities for pupils learning and will, in return, expect guest users to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that students / pupils receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

For my professional and personal safety:

- I understand that the academy will monitor my use of academy digital technology and communications systems.

- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email, VLE etc.) out of school, and to the transfer of personal data (digital or paper based) out of school.
- I understand that academy digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school. (schools should amend this section in the
- light of their policies which relate to the personal use, by guest users, of academy systems)
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using academy ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the Trust policy on the use of digital / video images.
- I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the Trust / academy websites / Teams) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use social networking sites in school in accordance with the Trust's policies.
- I will only communicate with students / pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The Trust have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the academy:

- When I use my mobile devices (laptops / tablets / mobile phones / USB devices etc.) in school, I will follow the rules set out in this agreement, in the same way as if I was using academy equipment. I will also follow any additional rules set by the school / academy about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not use personal email addresses on the academy ICT systems.

- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programs)
- I will ensure that my data is regularly backed up, in accordance with relevant academy policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programs or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programs of any type on a machine, or store programs on a computer, nor will I try to alter computer settings, unless this is allowed in school / academy policies.
- I will not disable or cause any damage to academy equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the Trust Data Protection Policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based Protected and Restricted data must be held in lockable storage.
- I understand that data protection policy requires that any guest users or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by Trust policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for academy sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of the academy:

- I understand that this Acceptable Use Policy applies not only to my work and use academy digital technology equipment in school, but also applies to my use of academy systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the academy

- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors / Executive Leadership Team and Trustees, and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use academy digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the Trust / academy) within these guidelines.

Guest User Name: ……

Signed: ……

Date: ……

Reporting Log

Academy:

Date	Time	Incident	Action Taken		Incident Reported By	Signature
			What?	By Whom?		

Training Needs Audit Log

Academy:

Relevant training the last 12 months	Identified Training Need	To be met by	Cost	Review Date
