Fairfield
Farm
College

E-Safety & Online Protection Policy

Policy number	New or Reviewed	Date of next review	Responsibility
PO17	September 2018	September 2019	Director of Education

To provide young people with opportunities to be successful and make a positive contribution within their community.

Fairfield
Farm
Trust
Charity No. 273924

1. Rationale

New technologies have become integral to the lives of young people in today's society, both within colleges and in their lives outside college.

The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and learners learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

There may be times when professional judgement are made in situations not covered by this document, or directly contravene the standards outlined in this document. It is expected that in these circumstances that staff will advise the Principal of any such action. The Principal will in turn seek advice and log any activity.

The requirement to ensure that young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of this policy. A college e-safety policy helps to ensure safe and appropriate use. The development and implementation of such a strategy should involve all the stakeholders in the young person's education from the Principal and Trustees to the senior leaders and tutors, support staff, parents, members of the community and the learners themselves.

The use of these exciting and innovative tools in college and at home has been shown to raise educational standards and promote learner / learner achievement.

However, the use of these new technologies can put young people at risk within and outside the college. Some of the dangers they may face include:

- Access to illegal, harmful, unsuitable or inappropriate content.
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Cyber-bullying
- Access to poor quality, inaccurate and irrelevant information
- Plagiarism and copyright infringement
- Illegal file sharing
- Excessive use which may impact on the social and emotional development and learning of the young person

Many of these risks reflect situations in the off-line world and it is essential that this e-safety policy is used in conjunction with other college policies:

- Behaviour Policy
- Guidance for Safer Working Practice for Adults who work with Children and Young People
- Child Protection Policy
- Disciplinary Policy and Procedures
- Equal Opportunities Policy
- Health and Safety Policy
- Acceptable Use of ILT Policy

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build learners' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

Fairfield Farm College will demonstrate that it has provided the necessary safeguards to help ensure that they have done everything that could reasonably be expected of them to manage and reduce these risks. The e-safety policy that follows explains how we intend to do this, while also addressing wider educational issues in order to help young people (and their parents / carers) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

2. Scope of the Policy

This policy applies to all members of the college community (including staff, learners, volunteers, parents / carers, visitors and community users) who are users of college ILT systems including use on personal devices.

This policy is intended to help young people and colleagues to their use of Social media and the Internet both on and off the college site and empower members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to e-safety incidents covered by this policy, which may take place out of college, but is linked to membership of the college.

The college 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 e-safety behaviour that take place out of college.

This policy is designed to cover all technologies that are used within the College Community both on and off site.

3. Roles and Responsibilities

The following section outlines the roles and responsibilities for e-safety of individuals and groups within the college:

Senior Leadership

- The Principal and is responsible for ensuring the safety (including e-safety) of members of the college community, though the day to day responsibility for e-safety will be delegated to all staff.
- The Senior Leadership Team are responsible for ensuring that the tutors and other relevant staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as relevant
- The Senior Leadership Team Leaders will ensure that there is a system in place to support and regulate those in college who carry out the internal e-safety monitoring role.
- The Principal and another member of the Senior Leadership Team are aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.

IT Manager

The IT Manager is responsible for ensuring:

- That the college's ILT infrastructure is secure and is not open to misuse or malicious attack
- That the college meets the e-safety technical requirements outlined in the relevant policies
- That users may only access the college's networks through a properly enforced password protection policy, in which passwords are regularly changed
- The college filtering policy is applied and reviewed on a regular basis and that its implementation is the responsibility of all users.
- That he / she keeps up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant
- That the use of the network / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the ILT Manager for investigation, action or sanction
- That monitoring software / systems are implemented and updated as agreed in college policies

Members of the College Community

Are responsible for ensuring that:

- Their actions, behaviour and conduct should avoid any reasonable person to question their motivation and intentions.
- They work and should be seen to work in an open and transparent way.
- They continually monitor and review their practice in terms of the evolving world of learning technologies

- They have an up to date awareness of e-safety matters and of the current college e-safety policy and practices
- They have read, understood and signed the college Staff Acceptable Use Policy
- They report any suspected misuse or problem to their Line Manager for investigation, action or sanction
- E-safety issues are embedded in all aspects of the curriculum and other college activities
- Learners understand and follow the college e-safety and acceptable use policy
- Learners have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- They monitor ILT activity in lessons, extracurricular and extended college activities
- They are aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current college policies with regard to these devices
- In lessons where internet use is pre-planned learners 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

Safeguarding Team/Designated Lead

Should be trained in e-safety issues (in particular specific online safety training for DSLs (KCSIE 2018) and be aware of the potential for serious child protection 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
- Cyber-bullying
- Exploitation and other risky behaviours using online resources.

It is important to emphasise that these are child protection and serious safeguarding issues, not technical issues and that technology provides additional means for child protection issues to develop.

The Safeguarding Team should also:

- Take day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the college e-safety policies / documents
- Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- Provides training and advice for staff
- Liaises with all relevant parties
- Meets when appropriate with the IT Manager to discuss current issues, review incident logs and filtering / change control logs
- Reports regularly to Senior Leadership Team

4. Policy Statements

Education – Learners

Whilst regulation and technical solutions are very important, their use must be balanced by educating learners to take a responsible approach. The education of learners in e-safety is therefore an essential part of the college's e-safety provision. Young people need the help and support of the college to recognise and avoid e-safety risks and build their resilience.

E-Safety education will be provided in the following ways:

- e-safety will be embedded into the tutorial and also through each young person's activities across college. This focus will cover both the use of ILT and new technologies in college and outside college
- Key e-safety messages should be reinforced as part of tutorial / pastoral activities across the whole college.
- Learners 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
- Learners should be helped to understand the need for the learner / learner AUP and encouraged to adopt safe and responsible use of ILT, the internet and mobile devices both within and outside college
- Learners should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Rules for use of ILT systems / internet will be displayed in learning areas and at the time of login.
- The college uses software to monitor and protect young people form accessing inappropriate content, however, in addition, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, learners may need to research topics (e.g. sexual health, drugs, and extremism) that would normally result in internet searches being blocked. In such a situation, staff can request that the IT Manager (and other relevant person) can temporarily remove those sites from the filtered list. This is provided that the activity is monitored and supervised by a staff member.
- Learners should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

Education – Parents / Carers

Many parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / 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.

Education & Training – Staff

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

- A planned programme of formal e-safety training will be made available to staff. Ongoing e-safety training needs of all staff will be carried out regularly. It is expected that some staff will identify e-safety as a training need within the performance management process.
- All new staff should receive e-safety guidance as part of their induction programme, ensuring that they fully understand the college e-safety policy and Acceptable Use Policies
- All staff will take precautions that keep themselves and others safe: not using personal devices whilst on duty; ensuring that any personal information publicly broadcasted through social media, such as Twitter is protected by the highest security settings available and will not use the College's name in any posting without consent of the SLT.

Technical – infrastructure / equipment, filtering and monitoring

- The college will be responsible for ensuring that the college 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 named in the above sections will be effective in carrying out their e-safety responsibilities:
- College ILT systems will be managed in ways that ensure that the college meets the e-safety technical requirements outlined in this policy.
- There will be regular reviews and audits of the safety and security of college ILT systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to college ILT systems. Details of the access rights available to groups of users will be recorded by the IT Manager and will be reviewed annually
- All users will be provided with a username and password where appropriate by the IT Manager who will keep an up to date record of users and their usernames. Users will be allowed to change their password regularly. Use by learners in this way should always be supervised and members of staff should never use a class log on for their own network access.
- 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. Staff may not also use others' designated IT equipment without permission.
- The college maintains and supports the managed filtering service.
- Any filtering issues should be reported immediately to IT Manager
- Requests from staff for sites to be removed from the filtered list will be considered by the IT Manager. A log will be kept of these and those requesting such action.

- The IT Manager regularly monitors and records the activity of users on the college ILT systems and users are made aware of this in the Acceptable Use Policy.
- Remote management tools are used by staff to control workstations and view users' activity
- Users must report any actual / potential e-safety incident to the IT Manager
- 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 college systems and data.
- Guests are given access to the college network with the same rights as a learner. The wireless password is changed regularly.
- Fairfield Farm College operates a policy of restricting the ability of all users to download, save and run executable files from the internet or removable media
- An agreed policy is in place regarding the extent of personal use that users and their family members are allowed on laptops and other portable devices that may be used out of college.
- Fairfield Farm College forbids staff from installing programmes on college workstations / portable devices, without the prior consent of the IT Manager.
- Fairfield Farm College allows the use of removable media (e.g. memory sticks / CDs / DVDs) by users on college workstations / portable devices in agreement with the IT manager. This information will be encrypted and all staff have the responsibility to ensure that this happens. If in doubt, the IT manager will assist. Personal data cannot be sent over the internet or taken off the college site unless safely encrypted or otherwise secured.

5. Use of Digital Media - Photographic, Video and Audio

Staff and learners need to be aware of the risks associated with sharing digital media. This media may remain available accessible and may cause harm or embarrassment to individuals in the short or longer term. The college will inform and educate users about these risks and will implement policies to reduce the potential for harm:

- When using digital images, staff should inform and educate learners 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.
- Staff are allowed to record digital media (using devices supplied by the College only) to support educational aims, but must follow college policies concerning the sharing, distribution and publication of the media
- Care should be taken when recording digital media that learners are appropriately dressed and are not participating in activities that might bring the individuals or the college into disrepute
- Learners must not take, use, share, publish or distribute images of others without appropriate permission
- Photographs published on the website, or elsewhere that include learners will be selected carefully and will comply with good practice guidance on the use of such images.
- Learners' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before digital media recordings of learners are published publicly, including social media.
- If the college does not have permission to use digital recordings publicly, then this will be adhered to. The use of digital recordings as part of the learners' programme, for accreditation and evidence tracking is permissible as these are for internal use.

6. GDPR

- Personal data will be recorded, processed, transferred and made available according to the GDPR (2018) regulation that require due attention to:
    - **Lawful, fair and transparent processing**
    - **Limitation of purpose, data and storage**
    - **Data subject rights**
    - **Consent**
    - **Personal data breaches**
    - **Privacy by Design**
    - **Data Protection Impact Assessment**
    - **Data transfers**
    - **Data Protection Officer**
    - **Awareness and training**

Staff must ensure that they:

- At all times take care to ensure the safe keeping of data, minimising the risk of its loss or misuse.
- Use data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" or "locked" when leaving the device.
- Transfer data using encryption and secure password protected devices.

When personal data is stored on any device or external media:

- The device must be encrypted or password protected.
- The device must not compromise the security of the college system. If in doubt it is the responsibility of the individual to liaise with the IT manager to ensure compliance
- The data must be securely deleted from the device once it has been transferred or its use is complete

7. Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the college manages the risks of new and innovative technologies.

Staff & other adults

- Personal devices and technology provided by the college can be used by learners as part of the planned learning programme. This use will still be governed by the guidance in this policy. Personal devices may not be used to take pictures of others without consent. These images/recordings may not be shared publicly.
- The use of personal devices by staff during work hours is not permissible.
- Staff devices must not be used to record images of learners under any circumstances.
- The use of college devices to access sensitive or personal information in public areas is not permitted.

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

- Adults within the college should always maintain appropriate professional boundaries and avoid behaviour, during their use of the internet and other communication technologies, which could be misinterpreted. They should report any incident with this potential to the IT Manager who will record as appropriate
- In their own interests, adults within college settings need to be aware of the dangers of sharing personal information. Information that could identify your profession or the college where you work should be protected
- All adults, particularly those new to the college, should review any personal information in the public domain to ensure that the information is accurate and appropriate. This includes any photographs that may cause embarrassment to themselves and the college

- Adults need to ensure that when they are communicating about others, even outside of college, that they give due regard to the potential for defamation of character and comply with requirements of equalities legislation
- Adults must never post derogatory remarks or offensive comments on-line or engage in on-line activities which may bring the college into disrepute or reflect negatively on their professionalism
- The official college email service may be regarded as safe and secure and is monitored. Staff and learners should therefore use only the college email service to communicate with others when in college, or on college systems (e.g. by remote access).
- Users need to be aware that electronic communications are monitored
- Users must immediately report, to the nominated person – in accordance with the college policy, the receipt of any electronic communication 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 learners or parents / carers (such as email) must be professional in tone and content. Under no circumstances, should staff accept friend requests on social media; share their personal phone numbers, contact details with learners.
- Adults should refrain from accepting requests from ex-learners where a link with the college community is maintained
- Personal email addresses, text messaging, mobile phones or public chat / social networking programmes must not be used for communications regarding the college; its business or its learners.
- Learners should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
- Personal information should not be posted on the college website and only official email addresses should be used to identify members of staff.
- There will be occasions when there are social contacts between learners and staff, where for example the parent and teacher are part of the same social circle. These contacts should be openly acknowledged and recorded by the IT Manager where there may be implications for the adult and their position within the college

8. Unsuitable / Inappropriate Activities

The college believes that the activities referred to in the following section would be inappropriate in a college context and that users, (learners, visitors, staff or parents), should not engage in these activities in college or outside college when using college equipment or systems.

The college policy restricts certain internet usage as follows:

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
- Promote or conduct of illegal acts, e.g. under the child protection, obscenity, computer misuse and fraud legislation
- Access or engage in:
    - any adult material that potentially breaches the Obscene Publications Act in the UK
    - criminally discriminatory material in UK
    - Pornography
    - promotion of any kind of discrimination
    - promotion of racial or religious hatred
    - threatening behaviour, including promotion of physical violence or mental harm
    - any other information which may be offensive to colleagues or breaches the integrity of the ethos of the college or brings the college into disrepute
    - Using college systems to run a private business
    - Use systems, applications, websites or other mechanisms that bypass the monitoring or other safeguards employed by the college
    - Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions
    - Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)
    - Creating or propagating computer viruses or other harmful files
    - Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet
    - On-line gaming (educational)
    - On-line gaming (non educational)
    - On-line gambling X On-line shopping / commerce
    - File sharing
    - Use of social networking sites
    - Use of video broadcasting

9. Responding to incidents of misuse

It is expected that all members of the college community are responsible users of ILT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through misadventure, careless or irresponsible use or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse for most members of the college community. When dealing with incidents the IT Manager will liaise with people involved and identify if the response is appropriate and proportionate.

If any apparent or actual misuse appears to involve illegal activity, as previously identified, the It Manager/Principal should be consulted and actions followed in line with the flow chart, in particular the sections on reporting the incident to the police and the preservation of evidence.

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 college 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 college community are aware that incidents have been dealt with.

It is intended that incidents of misuse will be dealt with through college behaviour policy or Disciplinary Policies and Procedures.

10. Sanctions

- Refer to IT Manager/HR Disciplinary/AuP
- Removal of access
- Refer to Police
- Refer for action re filtering / security etc.
- Removal of network / internet access rights
- Warning Further sanction, suspensions, exclusion

Examples of misuse that would warrant sanctions include, but are not limited to:

- Unauthorised use of non-educational sites during lessons
- Unauthorised use of mobile phone / digital camera / other handheld device
- Unauthorised use of social networking / instant messaging / personal email
- Unauthorised downloading or uploading of files
- Allowing others to access college network by sharing username and passwords
- Attempting to access or accessing the college network, using another learner's / learner's account
- Attempting to access or accessing the college network, using the account of a member of staff
- Corrupting or destroying the data of other users
- Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature
- Continued infringements of the above, following previous warnings or sanctions
- Actions which could bring the college into disrepute or breach the integrity of the ethos of the college
- Using proxy sites or other means to subvert the college's filtering system
- Accidentally accessing offensive or pornographic material and failing to report the incident
- Deliberately accessing or trying to access offensive or pornographic material

- Receipt or transmission of material that infringes the copyright of another person or infringes GDPR.
- Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email
- Unauthorised downloading or uploading of files
- Allowing others to access college network by sharing username and passwords or attempting to access or accessing the college network, using another person's account
- Careless use of personal data e.g. holding or transferring data in an insecure manner
- Deliberate actions to breach data protection or network security rules
- Corrupting or destroying the data of other users or causing deliberate damage to hardware or software
- Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with learners
- Actions which could compromise the staff member's professional standing

11. Learner Acceptable Use Policy Agreement (a copy to signed by all learners)

I understand that I must use college ILT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ILT systems and other users.

For my own personal safety:

- I understand that the college will monitor my use of the ILT systems, email and other digital communications.
- I will treat my username and password like my toothbrush – I will not share it, nor will I try to use any other person's username and password.
- I will be aware of "stranger danger", when I am communicating on-line.
- I will not disclose or share personal information about myself or others when on-line.
- I will not arrange to meet people off-line that I have communicated with on-line.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.
- I understand that everyone has equal rights to use technology as a resource and:
- I understand that the college ILT systems are primarily intended for educational use and that I will not use the systems for personal or recreational use unless I have permission to do so.
- 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 use the college ILT systems for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (e.g. YouTube), unless I have permission of a member of staff to do so.
- I will act as I expect others to act toward me:
- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images, video or audio recordings of anyone without their permission
- I recognise that the college has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the college:
- I will only use my personal hand held / external devices (mobile phones / USB devices/laptops etc.) in college if I have permission. I understand that, if I do use my own devices in college, I will follow the rules set out in this agreement, in the same way as if I was using college equipment.
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to

bypass the filtering / security systems in place to prevent access to such materials.

- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any attachments to emails, unless I know and trust the person / organisation who sent the email, due to the risk of the attachment containing viruses or other harmful programmes.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings.
- I will not use personal chat and social networking sites in college
- I will never invite staff to join my profile.

When using the internet for research or recreation, I recognise that:

- I should 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 try to download copies (including music and videos)
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

I understand that I am responsible for my actions, both in and out of college:

- I understand that the college also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of college and where they involve my membership of the college community (examples would be cyber-bullying, use of images or personal information).
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may include loss of access to the college network / internet, detentions, suspensions, contact with parents and in the event of illegal activities involvement of the police.

Name of Young Person:

Signature: Date:

12. Staff Acceptable Use of Internet and ILT Policy (A copy to be signed by all staff)

New technologies have become integral to the lives of children and young people in today's society, both within colleges and in their lives outside college. 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, efficient and productive in their work. All users should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- That staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- That college ILT 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 ILT in their everyday work.

The college will try to ensure that staff and volunteers will have good access to ILT to enhance their work, to enhance learning opportunities for learners learning and will, in return, expect staff and volunteers to agree to be responsible users.

Staff Acceptable Use of Internet & ILT Policy Agreement

I understand that I must use college ILT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ILT systems and other users. I recognise the value of the use of ILT for enhancing learning and will ensure that learners receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ILT and embed e-safety in my work with young people.

For my professional and personal safety:

- I understand that the college will monitor my use of the ILT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to the professional use of any College or Personal ILT Devices
- I understand that the college ILT 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 college
- I will not disclose my username or password to anyone else, nor will I try to use any other devices, person's username and password
- I will immediately report any illegal, inappropriate or harmful material or incident I become aware of, to the Principal

I will be professional in my communications and actions when using college ILT 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 college's policy on the use of digital media.
- I will not use my personal equipment to record images or video, unless an agreement has previously been made with the IT Manager. If this is the case I will make sure the media is deleted before the device is removed from the college site
- Where data is published it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use chat and social networking sites for college purposes, with permission.
- I will only communicate with learners and parents / carers using official college 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 college and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the college:
- When I use my personal hand held / external devices (PDAs / laptops / mobile phones / USB devices etc.) in college, I will follow the rules set out in this agreement, in the same way as if I was using college equipment. I will also follow any additional rules set by the college 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 take any confidential data offsite using an external device, or personal cloud based storage, unless the data or device has been encrypted by the network manager.
- I will not use personal email addresses for college communications
- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- I will ensure that my data is regularly backed up, in accordance with relevant college policies
- I will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer.
- I will not disable or cause any damage to college 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 College Data Protection Policy. Where personal data is transferred outside the secure college network, it must be encrypted.
- I understand that data protection policy requires that any staff or learner 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 college 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.
- I will ensure when logged in to the cloud services provided by the college that I treat the PC accessing these resources the same as I would in college (locking the PC when leaving it etc.)

When using the internet in my professional capacity or for college 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 college:
- I understand that this Acceptable Use Policy applies not only to my work and use of college ILT equipment in college, but also applies to my use of college ILT systems and equipment out of college and my use of personal equipment in college or in situations related to my employment by the college
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include normal disciplinary procedures and in the event of illegal activities the involvement of the police

I have read and understand the above and agree to use the college ILT systems and my own devices within these guidelines.

Staff / Volunteer Name..

Signed..

Date..

13. Consent for Photos & Videos of Learners taken at Fairfield Farm College (a copy to be signed by parents/guardians for all learners)

The use of images and video plays an important part in learning at Fairfield Farm College.

Learners and members of staff may use digital devices in lessons and to record evidence of learning, achievement and progress in lessons in and out of college. These images may then be used in presentations in subsequent lessons.

The college will comply with the GDPR and request parents / carers permission before publishing images of members of the college. We will also ensure that when images are published that the young people cannot be identified by the use of their names.

Parents and Carers are required to abide by the college's guidelines in the E-Safety policy (available from the college website or on request) when taking digital images at, or of, college events and when using digital images which include images of other children.

Parents and Carers are requested to sign the permission form below to allow the college to publish images of their children.

Photos & Videos Permission Form

Parent / Carers Name..

Learner Name..

As the parent / carer of the above learner, I agree to the college publishing images of my child/children. I understand that the images in publicity that reasonably celebrates success and promotes the work of the college.

Signed... Date ………………………………………….

14. Monitoring

. The college will therefore monitor the activities of users on the college network and on college equipment as indicated in the College E-Safety Policy and the Acceptable Use agreement.

Audit / Reporting

Logs of filtering change controls and of filtering incidents will be made available to:

- The DSL/SLT
- The IT Manager
- Local Authority on request
- Relevant authorities

The filtering policy will be reviewed in the response to the evidence provided by the audit logs of the suitability of the current provision.

15. College Password Security Policy

Introduction

The college will be responsible for ensuring that the college infrastructure / network is as safe and secure as is reasonably possible and that:

- users can only access data to which they have right of access
- No user should be able to access another's files, without permission (or as allowed for monitoring purposes within the college's policies).
- access to personal data is securely controlled in line with the college's personal data policy
- logs are maintained of access by users and of their actions while users of the system

A safe and secure username / password system is essential if the above is to be established and will apply to all college ILT systems, including email.

The management of the password security policy will be the responsibility of the IT Manager.

- All users (adults and young people) will have responsibility 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.
- Passwords for new users, and replacement passwords for existing users can be ILT Manager, Tutors and Directors/Admin.
- It is essential that users should be made aware of the need for keeping passwords secure, and the risks attached to unauthorised access / data loss. This should apply to everyone at FFC.

Members of staff will be made aware of the college's password policy:

- At induction
- Through the college's e-safety policy and password security policy
- Through the Acceptable Use Agreement

- All users will have clearly defined access rights to college ILT systems. Details of the access rights available to groups of users will be recorded by the IT Manager and will be reviewed at least annually.

All users will be provided with a username and password by the Network Manager who will keep an up to date record of users and their usernames.

The following rules apply to the use of passwords:

- Passwords will be forced to change regularly
- The last three passwords cannot be re-used
- The password should be a minimum of 7 characters long and
- Must include three of – uppercase character, lowercase character, number, special character
- The account will be "locked out" following 5 successive incorrect log-on attempts
- Temporary passwords e.g. used with new user accounts or when users have forgotten their passwords, shall be enforced to change immediately upon the next account log-on
- Passwords shall not be displayed on screen, and shall be securely hashed (use of one-way encryption)

16. College Personal Data Handling

Recent publicity about the loss of personal data by organisations and individuals has made this a current and high profile issue for colleges and other organisations. It is important that the college has a clear and well understood personal data policy because:

- No college or individual would want to be the cause of any loss of personal data, particularly as the impact of data loss on individuals can be severe and cause extreme embarrassment, put individuals at risk and affect personal, professional or organisational reputation.
- Colleges are "data rich" and the introduction of electronic storage and transmission of data has created additional potential for the loss of data
- The college will want to avoid the criticism and negative publicity that could be generated by any loss of personal data.
- The college is subject to a wide range of legislation related to data protection and data use, with significant penalties for failure to observe the relevant legislation.

Colleges have always held personal data on the learners in their care, and increasingly this data is held digitally and accessible not just in college but also from remote locations. Legislation covering the safe handling of this data is addressed by the GDPR (2018) Colleges should do everything within their power to ensure the safety and security of any material of a personal or sensitive nature.