Mill Chase Academy
E-Safety Policy

***Lead Governor:* Chair**

Senior Leadership Team Link: Steph Moral

Previous Review: October 2016

Next Review Due: January 2020

Ratified by Governors: 25th January 2018

This policy is part of the School's Statutory Safeguarding Policy. Any issues and concerns with online safety must follow the school's safeguarding and child protection processes.

1. Introduction and Overview

Rationale

The purpose of this policy is to:

- Set out the key principles expected of all members of the community at Mill Chase Academy with respect to the use of ICT-based technologies.
- Safeguard and protect the children and staff of Mill Chase Academy.
- Assist academy staff working with children to work safely and responsibly with the Internet and other communication technologies and to monitor their own standards and practice.
- Set clear expectations of behaviour and/or codes of practice relevant to responsible use of the Internet for educational, personal or recreational use.
- Have clear structures to deal with online abuse such as cyber-bullying.
- Ensure that all members of the academy community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- Minimise the risk of misplaced or malicious allegations made against adults who work with students.

Scope

This policy applies to all members of Mill Chase Academy (including staff, governors, students, volunteers, parents/carers, visitors) who have access to and are users of the academy IT systems, both in and out of Mill Chase Academy.

Role	Key Responsibilities
Principal	• Must be adequately trained in off-line and online safeguarding, in-line with statutory guidance and relevant Local Safeguarding Children Board (LSCB) guidance. • To lead a ‘safeguarding’ culture, ensuring that online safety is fully integrated with whole school safeguarding. • To take overall responsibility for online safety provision. • To take overall responsibility for data management and information security (SIRO) ensuring school’s provision follows best practice in information handling. • To ensure the school uses appropriate IT systems and services. • To be responsible for ensuring that all staff receive suitable training to carry out their safeguarding and online safety roles. • To be aware of procedures to be followed in the event of a serious online safety incident. • Ensure suitable ‘risk assessments’ undertaken so the curriculum meets the needs of students, including risk of children being radicalised. • To ensure that there is a system in place to monitor and support staff who carry out internal online safety procedures, e.g. network manager. • To ensure Governors are regularly updated on the nature and effectiveness of the school’s arrangements for online safety. • To ensure the school website includes relevant information.
Designated Safeguarding lead	• Take day to day responsibility for online safety issues and a leading role in establishing and reviewing the school’s online safety policy/documents. • Promote an awareness and commitment to online safety throughout the school community. • Ensure that online safety education is embedded within the curriculum. • Liaise with school technical staff where appropriate. • To ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident. • To ensure that online safety incidents are logged as a safeguarding incident. • Facilitate training and advice for all staff. • Oversee any student surveys / student feedback on online safety issues. • Liaise with the Local Authority and relevant agencies. • Is regularly updated in online safety issues and legislation, and be aware of the potential for serious child protection concerns.
Governors	• To ensure that the school has in place policies and practices to keep the children and staff safe online.

Role	Key Responsibilities
	• To approve the E-Safety Policy and review the effectiveness of the policy. • To support the school in encouraging parents and the wider community to become engaged in online safety activities. • The role of the safeguarding Governor will include: regular review with the Designated Safeguarding Lead.
Computing Curriculum Leader	• To oversee the delivery of the online safety element of the Computing curriculum. • To liaise with the Designated Safeguarding Lead regularly.
Network Manager	• To report online safety related issues that come to their attention, to the Designated Safeguarding Lead. • To manage the school's computer systems, ensuring: - School password policy is strictly adhered to. - Systems are in place for misuse detection and malicious attack (e.g. keeping virus protection up to date). - Access controls/encryption exist to protect personal and sensitive information held on school-owned devices. - The school's policy on web filtering is applied and updated on a regular basis. • That they keep up to date with the school's online safety policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant. • That the use of school technology and online platforms are regularly monitored and that any misuse/attempted misuse is reported to the Designated Safeguarding Lead & Principal. • To ensure appropriate backup procedures and disaster recovery plans are in place. • To keep up-to-date documentation of the school's online security and technical procedures.
Data and Information Manager	• To ensure that the data they manage is accurate and up-to-date. • Ensure best practice in information management, i.e. have appropriate access controls in place, that data is used, transferred and deleted in-line with data protection requirements.
All staff	• To embed online safety issues in all aspects of the curriculum and other academy activities. • To supervise and guide students carefully when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant). • To ensure that students are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws. • To read, understand and help promote the academy's online safety policies and guidance. • To read, understand, sign and adhere to the school staff Acceptable Use Agreement/Policy, and understand any updates annually. The AUP is signed by new staff on induction (see appendix 1).

Role	Key Responsibilities
	• To be aware of online safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current academy policies with regard to these devices. • To report any suspected misuse or problem to the Designated Safeguarding Lead. • To maintain an awareness of current online safety issues and guidance e.g. through CPD. • To model safe, responsible and professional behaviours in their own use of technology. • To ensure that any digital communications with students should be on a professional level and only through school based network systems, never through personal mechanisms, e.g. personal email, text, social media, mobile phones etc.
Pupils	• Read, understand, sign and adhere to the Student Acceptable Use Policy (see appendix 2). • To understand the importance of reporting abuse, misuse or access to inappropriate materials. • To know what action to take if they or someone they know feels worried or vulnerable when using online technology. • To know and understand academy policy on the use of mobile phones, digital cameras and hand held devices. • To know and understand academy policy on the taking/ use of images and on cyber-bullying. • To understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the academy's online safety policy covers their actions out of the academy, if related to their membership of the academy. • To take responsibility for learning about the benefits and risks of using the Internet and other technologies safely both in the academy and at home. • Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
Parents/carers	• To support the academy in promoting online safety. • To read and sign the Student Acceptable Use Agreement. • To consult with the academy if they have any concerns about their children's use of technology.

Communication:

The policy will be communicated to staff/students/community in the following ways:

- Policy to be posted on the academy website.
- Policy to be part of the annual safeguarding training.
- Acceptable use agreements to be issued, discussed and signed as part of the academy induction pack for new staff.

- Acceptable use agreements to be issued, discussed and signed with students on admission.
- Acceptable use agreements to be held in student and personnel files.
- Through the computing curriculum.
- Regular updates and training on online safety for all staff.

Handling incidents:

- The academy will take all reasonable precautions to ensure online safety.

- Staff and pupils are given information about infringements in use of the ICT systems and possible sanctions. Sanctions available include:
  - interview/monitoring by the Pastoral Support and Guidance Team/Mentor/Academic and Pastoral Leader/Designated Safeguarding Lead;
  - sanction through the normal routes of the academy behaviour policy;
  - informing parents or carers;
  - removal of internet or computer access for a period;
  - referral to Children's Services and/or the Police.

- Our Designated Safeguarding Lead acts as first point of contact for any incident. Any suspected online risk or infringement is reported to the Designated Safeguarding Lead that day.

- Our Designated Safeguarding Lead acts as first point of contact for any parental concern or complaint, who will discuss this matter with the Principal. Any incident about staff misuse is referred to the Principal unless the concern is about the Principal in which case the complaint is referred to the Chair of Governors and the LADO (Local Authority Designated Officer) in line with our child protection and safeguarding policies.

- Incidents of cyber-bullying are dealt with in accordance with our Anti-Bullying Policy and Behaviour Policy. Complaints related to child protection are dealt with in accordance with the academy child protection and safeguarding procedures.

- Any incident regarding the network system, for example - viruses, software, filtering systems, reported inappropriate material will be rectified and dealt with by the Network Manager in liaison with the senior leadership team.

Review and Monitoring

- The E-Safety policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the school.
- There is widespread ownership of the policy and it has been agreed by the SLT and approved by Governors. All amendments to the school online safety policy will be disseminated to all members of staff and pupils.

2. Education and Curriculum

Student online safety curriculum

This academy:

- Has a clear, progressive online safety education programme as part of the Computing curriculum, Experience Days/PSHE curriculum, mentoring programme and assembly programme. This policy covers a range of skills and behaviours appropriate to the age and experience of the academy's students, including:
    - to STOP and THINK before they CLICK
    - to develop a range of strategies to evaluate and verify information before accepting its accuracy;
    - to be aware that the author of a web site/page may have a particular bias or purpose and to develop skills to recognise what that may be;
    - to understand acceptable behaviour when using an online environment/email, i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private;
    - to understand how photographs can be manipulated and how web content can attract the wrong sort of attention;
    - to understand why on-line 'friends' may not be who they say they are and to understand why they should be careful in online environments;
    - to understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure they have turned-on privacy settings;
    - to understand why they must not post pictures or videos of others without their permission;
    - to know not to download or install any unapproved software or any files;
    - to have strategies for dealing with receipt of inappropriate materials;
    - to understand why and how some people will 'groom' young people for sexual reasons;
    - to understand the impact of cyber-bullying, grooming, online radicalisation, sexting and trolling and know how to seek help if they are affected by any form of online harassment or bullying;
    - to know how to report any abuse including cyber-bullying; and how to seek help if they experience problems when using the Internet and related technologies, i.e. parent or carer, teacher or trusted staff member, or an organisation such as ChildLine or the CLICK CEOP button.

- Plans online use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.
- Will remind students about their responsibilities through a Student Acceptable Use Policy which every student will sign and agree to when they log on to the academy network.
- Ensures staff will model safe and responsible behaviour in their own use of technology during lessons.

Staff training

This academy:

- Makes training available to staff on online safety issues during annual safeguarding training.
- Provides, as part of the induction process, all new staff with information and guidance on the online policy and the academy's Acceptable Use Policies.

Parent awareness and training

This academy:

- Through parental meetings and the academy website, we offer advice and guidance for parents, including:
    - Introduction of the Acceptable Use Agreements to new parents, to ensure that principles of online safety behaviour are made clear;
    - Information leaflets; in academy newsletters; on the academy web site;
    - suggestions for safe internet use at home;
    - provision of information about national support sites for parents

3. Expected Conduct and Incident management

Expected conduct

In this academy, all users:

- Are responsible for using the school IT systems in accordance with the relevant Acceptable Use Policy which they will be expected to sign before being given access to the academy systems.
- Need to understand the importance of misuse or access to inappropriate materials and are aware of the consequences.
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Should understand the importance of adopting good online safety practice when using digital technologies in and outside of the academy.
- Will be expected to know and understand academy policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand academy policies on the taking/use of images and on cyber-bullying.

Staff

- Know to be vigilant in the supervision of children at all times.
- Know to take professional, reasonable precautions when working with pupils, previewing websites before use; using age-appropriate (pupil friendly) search engines etc.
- Are responsible for using the academy IT systems accordingly, including the use of mobile phones, and hand held devices.
- Will understand their responsibilities through reading, signing and adhering to the Staff Acceptable Use Policy and which they will agree to when they log on to the academy network.

Students

- Should have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- Will understand their responsibilities through reading, signing and adhering to the Student Acceptable Use Policy and which they will agree to when they log on to the academy network.

Parents/Carers

- Should provide consent for students to use the Internet, as well as other technologies, as part of the online safety Student Acceptable Use agreement form at the time of their child's entry to the academy.
- Should know and understand what the rules of appropriate use are and what sanctions result from misuse from reading the Student Acceptable Use Policy.

Incident Management

In this academy:

- There is strict monitoring and application of the online safety policy and a differentiated and appropriate range of sanctions.
- All members and the wider community are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively.
- Support is actively sought from other agencies as needed (e.g. the Local Authority, UK Safer Internet Centre, Police, CEOP and Think U Know) in dealing with e-safety issues.
- Monitoring and reporting of online safety incidents takes place and contribute to developments in policy and practice in online safety within the academy.
- Parents/carers are specifically informed of online safety incidents involving young people for whom they are responsible.
- We will contact the Police if one of our staff or students receives online communication that we consider is particularly disturbing or breaks the law.
- We will immediately refer any suspected illegal material to the appropriate authorities.
- Our Designated Safeguarding Lead acts as first point of contact for any child protection or safeguarding incident.
- Any incident about staff misuse is referred to the Principal unless the concern is about the Principal in which case the complaint is referred to the Chair of Governors and the LADO (Local Authority Designated Officer) in line with our child protection and safeguarding policies.
- Incidents of cyber-bullying are dealt with in accordance with our Anti-Bullying Policy and Behaviour Policy.
- Any incident regarding the network system, for example - viruses, software, filtering systems, reported inappropriate material will be rectified and dealt with by the Network Manager in liaison with the senior leadership team.

4. Managing the ICT infrastructure

Internet access, security (virus protection) and filtering

This academy:

- Uses Virgin Media as the Internet Provider.
- Uses the filtering system supplied by Hampshire County Council Hosted School Service (HSS).
- Uses the Hampshire County Council secure email system in relation to sending and receiving information and documents regarding child protection.
- Is vigilant in its supervision of student use at all times, as far as is reasonable.
- Ensures all staff and students have signed an acceptable use agreement form and understand that they must report any concerns.
- Informs all users that Internet/email use is monitored.
- Informs staff and students that that they must report any failure of the filtering systems directly to the Network Manager.
- Makes clear all users know and understand what the 'rules of appropriate use' are and what sanctions result from misuse through the acceptable use agreements, staff meetings and teaching programme.
- Provides advice and information on reporting offensive materials, abuse/ bullying etc. available for pupils, staff and parents.
- Immediately refers any material we suspect is illegal to the appropriate authorities.

Network management

This academy:

- Uses individual log-ins for all users.
- Uses guest accounts for external or short term visitors for temporary access to appropriate services.
- Uses teacher 'remote' management control tools for controlling workstations / viewing users / setting-up applications and Internet web sites, where useful.
- Has additional local network auditing software installed.
- Has daily back-up of school data.
- Ensures the Systems Administrator/Network Manager is up-to-date with Hampshire IT services and policies.
- Ensures all data stored on the system within the academy conforms to the UK data protection requirements.

To ensure the network is used safely

This academy:

- Ensures staff and students read and sign that they have understood the academy's Acceptable Use Policy. Following this, they are set-up with Internet, email access and network access. Access to the academy service is through a unique username and password.
- Ensures staff access to the academy's management information system is controlled through a separate password for data security purposes.

- Ensures students must not join a newsgroup, mailing lists or chat room. If any other user wishes to join a newsgroup, mailing list, or chat room, permission must be sought from the Computing HOD or Principal.

- Ensures the Internet and email are used legally and responsibly. A user must not do anything that could expose students to any risks, bring the academy into disrepute, cause offence, cause damage or jeopardise the security of data, networks, equipment or software, or break laws such as copyright and data protection.

- Requests that use of the Internet should be supervised at all times by a member of staff.

- Ensures all use of the Internet will be monitored and computers on the network will be interrogated to ensure that use of the Internet has been appropriate and abides by the Internet policy.

- Requests that any user that comes across offensive or illegal material should immediately inform the Network Manager who will inform the Designated Safeguarding Lead for action to be taken.
- Makes clear that no one should log on as another user and makes clear that students should never be allowed to log-on or use teacher and staff logins as these have far less security restrictions and inappropriate use could damage files or the network.
- Has set-up the network with a work area for students and one for staff. Staff and students are shown how to save work and access work from these areas.
- Requires all users to always log off or lock the computer when they have finished working or are leaving the computer unattended.

- Where a user finds a logged-on machine, we require them to always log-off and then log-on again as themselves.
- Has set-up the network so that users cannot download executable files/ programmes.
- Scans all mobile equipment with anti-virus/spyware before it is connected to the network.
- Makes clear that staff are responsible for ensuring that all equipment that goes home has the anti-virus and spyware software maintained up-to-date and the academy provides them with a solution to do so.
- Makes clear that staff are responsible for ensuring that any computer or laptop loaned to them by the academy is used solely to support their professional responsibilities.
- Maintains equipment to ensure Health and Safety is followed.

- Ensures that access to the academy’s network resources from remote locations by staff is restricted and access is only through academy / Local Authority approved systems – crypto card.
- Does not allow any outside agencies to access our network remotely except where there is a clear professional need and then access is restricted and is only through approved systems; e.g. technical support or MIS Support.
- Makes clear responsibilities for the daily back up of MIS and finance systems and other important files.

- Has a clear disaster recovery system in place for critical data that includes a secure, remote back up of critical data, which complies with external Audit's requirements.
- Uses our broadband network for our CCTV system and have had set-up by approved partners.
- Uses the DfE secure s2s website for all CTF files sent to other schools.
- Ensures that all student level data or personal data sent over the Internet is encrypted or only sent within the approved secure system in our Local Authority.
- Follows ISP advice on Local Area and Wide Area security matters and firewalls and routers have been configured to prevent unauthorised use of our network.
- Our wireless network has been secured to industry standard Enterprise security level /appropriate standards suitable for educational use.
- Projectors are maintained so that the quality of presentation remains high.
- All IT and communications systems installed professionally and regularly reviewed to ensure they meet health and safety standards.

Access and Passwords

In this academy:

- All staff and students have their own unique username and passwords to access academy systems. They are responsible for always keeping their username and password private. They must not share it with others and must not leave it where others can find it.
- The system requires staff to change their password frequently.
- All staff and students sign and agree to the Acceptable Use Policy.

E-mail

This academy:

- Provides staff and students with an email account for their professional and educational use.
- We use anonymous or group e-mail addresses, for example enquiries@millchase.hants.sch.uk for communication with the wider public.
- Informs students that they may only use the approved e-mail accounts on the system. When communicating by e-mail, students must not reveal their personal details or those of others, or arrange to meet anyone without specific permission. Students must immediately tell a member of staff if they receive an offensive e-mail.
- Will contact the Police if one of our staff or students receives an e-mail that we consider to be particularly disturbing or breaks the law.
- Will ensure that email accounts are maintained and up to date.
- Reports messages relating to or in support of illegal activities to the relevant authority and if necessary to the Police.

- Knows that spam, phishing and virus attachments can make e-mails dangerous. We use a number of technologies to help protect users and systems in the academy for filtering, protecting and monitoring.

Students:

- Students are introduced to, and use e-mail as part of the IT/Computing scheme of work.
- Students are taught about the safety and appropriate use of using e-mail both in the academy and at home i.e. they are taught:
    - not to give out their e-mail address unless it is part of an academy managed project or to someone they know and trust and is approved by their teacher or parent/carer;
    - to treat others with respect and only use language that will not cause upset ot harm in any communication;
    - they must not reveal private details of themselves or others in e-mail, such as address, telephone number, etc;
    - to 'Stop and Think Before They Click' and not open attachments unless sure the source is safe;
    - that they should think carefully before sending any attachments;
    - that they must immediately tell a teacher / responsible adult if they receive an e-mail which makes them feel uncomfortable, is offensive, is harassment, is requesting them to do something inappropriate or is bullying in nature;
    - not to respond to malicious or threatening messages;
    - not to delete malicious of threatening e-mails, but to keep them as evidence of bullying;
    - not to arrange to meet anyone they meet through e-mail without having discussed with an adult and taking a responsible adult with them;
    - that forwarding 'chain' e-mail letters is not permitted.

- Students sign the academy Acceptable Use Policy to say they have read and understood the online safety rules, including e-mail and we explain how any inappropriate use will be dealt with.

Staff:

- All staff sign the academy Acceptable Use Policy to say they have read and understood the online safety rules, including e-mail and we explain how any inappropriate use will be dealt with.

Academy website

- The Principal takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained.
- The academy website complies with the statutory DfE requirements.
- Most material is the academy's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status.
- The point of contact on the web site is the school address and telephone number and we use a general email contact address, e.g. enquiries@millchase.hants.sch.uk.

- Photographs published on the web do not have full names attached.
- We do not use students' names when saving images in the file names or in the tags when publishing to the academy website.

Social networking

- Staff are instructed to always keep professional and private communication separate.
- Teachers are instructed not to run social network spaces for student use on a personal basis or to open up their own spaces to their students or parents, but to use the academy preferred system for communications (academy network).
- Staff will ensure that in private use:
    - No reference should be made in social media to students, parents/carers or academy staff;
    - They do not engage in online discussion on personal matters relating to the academy community or members of the academy community;
    - School staff should not be online friends with any pupil/student. Any exceptions must be approved by the Principal.
    - Personal opinions should not be attributed to the academy, academy trust or local authority and personal opinions must not compromise the professional role of the staff member, nor bring the school into disrepute;
    - Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

- Students are taught about social networking, acceptable behaviours and how to report misuse, intimidation or abuse through our online safety curriculum work.
- Students are required to sign and follow our student Acceptable Use Agreement.
- Parents are reminded about social networking risks and protocols through our student Acceptable Use Agreement and additional communications materials when required.

CCTV and Recordings

We have CCTV in the academy as part of our site surveillance for staff and student safety. We will not reveal any recordings without permission except where disclosed to the Police as part of a criminal investigation.

We use specialist lesson recording equipment on occasions as a tool to share best teaching practice. We do not reveal any such recordings outside of the staff and will not use for any other purposes.

5. Data security: Management Information System access and Data transfer

Strategic and operational practices

At this academy:

- The Principal is the Senior Information Risk Officer (SIRO).

- We ensure staff know who to report any incidents where data protection may have been compromised.
- All staff are DBS checked and records are held in one central record.
- We ensure all students and staff sign an Acceptable Use Policy agreement. We have a system so we know who has signed.
- We follow Local Authority guidelines for the transfer of any data, such as MIS data or reports of children, to professionals working in the Local Authority or their partners in Children's Services / Family Services, Health, Welfare and Social Services.
- We require that any Protect and Restricted material must be encrypted if the material is to be removed from the academy and limit such data removal. We have an approved remote access solution so staff can access sensitive and other data from home, without need to take data home. This is a remote system via crypto card – we can supply encrypted memory sticks if required.

Technical Solutions

- Staff have secure area(s) on the network to store sensitive documents or photographs.
- We require staff to log-out of systems when leaving their computer, but also enforce lock-out after one hour idle time to allow no disruption to lessons.
- We can supply encrypted flash drives if required to allow any member of staff to take any sensitive information off site.
- We use the DfE S2S site to securely transfer CTF pupil data files to other schools.
- We use the Hampshire Admissions system to transfer admissions data.
- We use the Hampshire crypto card for remote access into our systems.
- We use Hampshire HSS to transfer other data to schools, such as references, reports of children.
- We use Hampshire HSS secure data transfer system, for creation of online user accounts for access to broadband services.
- We store any Protect and Restricted written material in lockable storage cabinets in a lockable storage area.
- All servers are in lockable locations and managed by DBS-checked staff.
- We use Hampshire HSS remote secure back-up for disaster recovery on our network / admin, curriculum server(s).
- We use and comply with Hampshire HSS to dispose of equipment and to wipe data. The academy will obtain certificates of deletion of data if disposing of own equipment.
- Portable equipment loaned by the academy (for use by staff at home), where used for any protected data, is disposed of through Hampshire HSS.
- Paper based sensitive information is shredded and / or collected by secure data disposal service supplied by Hampshire HSS.
- We are using secure file deletion software supplied by Hampshire HSS.

6. Equipment and Digital Content

Personal mobile phones and mobile devices

- Mobile phones and personally-owned mobile devices brought in to the academy are the responsibility of the device owner. The academy accepts no responsibility for the loss, theft or damage of personally-owned mobile phones or mobile devices.
- Student mobile phones which are brought into the academy must not be used for calling or texting at all during the school day. They are for emergency use to and from the academy only. They can be used at break or lunchtime for the purpose of listening to music through headphones.
- Staff members may use their phones during school break times.
- The recording, taking and sharing of images, video and audio on any personal mobile phone is prohibited. Staff should only use academy devices for such activities.
- The academy reserves the right to search the content of any mobile or handheld devices on the academy premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying. Staff mobiles or hand held devices may be searched at any time as part of routine monitoring.
- Where parents or students need to contact each other during the school day, they should do so only through the academy office.
- Mobile phones and personally-owned devices are not permitted to be used in certain areas within the school site, e.g. changing rooms and toilets.
- Mobile phones will not be used during lessons or formal school time unless as part of an approved and directed work/curriculum-based activity with consent from a member of staff.

- The Bluetooth or similar function of a mobile phone should be switched off at all times and not be used to send images or files to other mobile phones.
- Personal mobile phones will only be used during lessons with permission from the teacher.
- No images or videos should be taken on mobile phones or personally-owned mobile devices.

Students' use of personal devices

- If a student breaches the academy policy then the phone or device will be confiscated and will be held in a secure place in the school office for collection at the end of the day.
- Phones and devices must not be taken into examinations. Students found in possession of a mobile phone during an exam will be reported to the appropriate examining body. This may result in the student's withdrawal from either that examination or all examinations.
- If a student needs to contact his or her parents or carers, they will be allowed to use an academy phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the academy office.
- Students should protect their phone numbers by only giving them to trusted friends and family members. Students will be instructed in safe and appropriate use of mobile phones and personally-owned devices and will be made aware of boundaries and consequences.

Staff use of personal devices

- Staff members may use their phones during school break times.
- Staff are not permitted to use their own mobile phones or devices for contacting children, young people or their families within or outside of the setting in a professional capacity.
- Staff will be issued with a school mobile phone where contact with students, parents or carers is required e.g. on school trips or visits.
- If members of staff have an educational reason to allow children to use mobile phones or a personally-owned device as part of an educational activity then it will only take place when approved by the HOD or senior leadership team.
- Staff should not use personally-owned devices, such as mobile phones or cameras, to take photos or videos of students and will only use academy equipment for this purpose.
- If a member of staff breaches the academy policy then disciplinary action may be taken.
- Where staff members are required to use a mobile phone for school duties, for instance in case of emergency during off-site activities, or for contacting students or parents, then the academy mobile phone will be provided and used. In an emergency where a staff member doesn't have access to an academy-owned device, they should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes.

Digital images and video

In this academy:

- We ask parents to notify the academy office if they do not give permission for their child to be photographed or filmed for use on the academy web site, in the prospectus or in other high profile publications when their daughter/son joins the academy.
- Staff sign the academy's Acceptable Use Policy and this includes a clause on not using personal mobile phones/personal equipment for taking pictures of students.
- The academy blocks/filter access to social networking sites unless there is a specific approved educational purpose.
- Students are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.
- Students are taught that they should not post images or videos of others without their permission. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.

Appendix 1

Mill Chase Academy
Staff IT Network Acceptable Use Policy

To ensure that members of staff are fully aware of their professional responsibilities when using information systems and when communicating with students, they are asked to sign this code of conduct. Members of staff should consult the academy policy on Internet Use and E-Safety for further information and clarification.

- I understand that it is a criminal offence to use an academy ICT system for a purpose not permitted by its owner.
- I understand that I must not use the academy ICT system to access inappropriate content.
- I will respect system security and I will not disclose any password or security information to anyone other than an authorised system manager. I will not use anyone's account except my own.
- If I find an inappropriate website or content on the academy network I will inform the ICT department and Network Manager immediately with the full web address.
- I will report any incidents of concern regarding children's safety to the academy Designated Safeguarding Lead immediately.
- I will promote e-safety with students in my care and will help them to develop a responsible attitude to system use, communications and publishing.
- I will supervise and guide students carefully when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant).
- I will not use social media, private mobile phones or other private devices to contact students or parents. Contact will only be made through the academy school network routes – e.g. the academy email system or telephone for parents.
- I will not use private camera functions on mobile telephones or other devices to take images of colleagues or students. Only academy equipment will be used for this purpose.
- I will not accept friend requests from any students, ex-students or parents on any private social media account.
- As a member of the academy I will ensure that through social media in private use:
    - No reference will be made in social media to students, parents/carers or academy staff;

    - I will not engage in online discussion on personal matters relating to the academy community or members of the academy community;
    - Personal opinions will not be attributed to the academy, academy trust or local authority;
    - Security settings on personal social media profiles will be regularly checked to minimise risk of loss of personal information.
- When writing messages and using the internet to communicate with other people (e.g. email, forums etc) I will be professional at all times, I will treat others with respect and I will only use language that will not cause upset or harm.
- I will ensure that electronic communications with students such as email through the academy network are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.
- I will model safe, responsible and professional behaviour in my own use of technology.
- I will log off or lock the computer when I have finished working or I am leaving the computer unattended.
- Where I find a logged-on machine, I will always log-off and then log-on again as myself.
- I will not allow a student to log into my user area. I understand that I have access to sensitive data through my account.
- I will not allow a student to use a computer where I am logged in.
- I will ensure that personal data e.g. documents with student or staff names, addresses, D.O.B is stored securely and is used appropriately, whether in the academy or taken off the academy premises or accessed remotely. I will NOT store this on removable storage devices – e.g. laptops, USB drives or disc.
- I understand that academy information systems and hardware may not be used for private purposes without specific permission from the Principal.
- I understand that my use of academy information systems, Internet and email may be monitored and recorded to ensure policy compliance.
- I will not install any software or hardware without permission.
- I will respect copyright and intellectual property rights.
- I understand use for personal financial gain, gambling, political activity, advertising or illegal purposes is not permitted.
- I will treat all ICT equipment with care; I will ensure students treat equipment with the same care and respect.
- If a fault develops on any equipment I will contact the Network Manager through the academy reporting procedures.
- I will protect computers, laptops and whiteboards from spillages by eating and drinking well away from the equipment.
- I will not allow any student to tamper or adjust any connections to a computer or tamper with any hardware.
- The academy may exercise its right to monitor the use of the academy's information systems and Internet access, to intercept e-mail and to delete inappropriate materials where it believes unauthorised use of the academy's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

Please sign below to agree with the above conditions.

'I have read, understood and agree to abide by all of the above conditions stated in the Staff IT Network Acceptable Use Policy.'

Name (BLOCK CAPITALS): ____

Staff Signature: ____

Date: ____

Appendix 2

Mill Chase Academy
Student IT Network Acceptable Use Policy

The Acceptable Use Policy ensures students at Mill Chase are protected when using IT equipment provided by The Academy. The policy describes acceptable behaviour when using any device at the Academy including students own devices, brought in at their own risk.

Whilst the use of IT is a valuable educational resource it remains a privilege, not a right. This privilege can be withdrawn for any student. Below are the expectations at Mill Chase Academy:

- I will not share my login details with any other student (including my password). Likewise I will never use another student's login details to access the network.
- I understand that any network access must be appropriate to education.
- If I find a computer still logged in, I know I must logoff that account immediately with no attempt to access another student's files or email.
- If I witness misuse of the Academy network I will report this to the Network Manager or the Teacher of my class immediately.
- When using the internet to communicate with other people (e.g. Email, Forums etc) I will treat others with respect and report any cases of bullying immediately to the Network Manager or Teacher.
- When writing messages to other people I will only use language that will not cause upset or harm.
- Bringing files into school such as executables of any type is forbidden; I will not download or install any unapproved software, system utility or resources from the Internet.
- Copyright Law must not be breached. I will not copy, send or receive material owned by the Academy or other third parties.
- To stay safe when using the Internet I must not share personal information whilst using on line resources such as email, blogging, personal publishing or any form of messaging.
- Chain messages waste resources and I will not start nor take part in them.
- I will make no attempt to use the network irresponsibly or attempt to "hack" the system.
- Access to inappropriate content on the internet is filtered and monitored by the Academy. I will report any access to such content immediately whether it is by myself or a fellow student.

- If I break any rules related to the use of IT, I understand the Academy Behaviour policy will be applied in exactly the same way as it is in normal lessons.
- From time to time photos will be taken of pupils for publicity reasons. If my parent or guardian objects, they must let the school office know and I will absent myself from any such photo.

The Academy reserves the right to monitor all access to the IT resources, this may include;

- Log access to websites and student email.
- Removal of inappropriate material
- Deletion of unlawful or unauthorised text, imagery or sound
- Removal of login privileges where unauthorised use of the Academy's network may be taking place.

Please sign below to agree with the above conditions. Your parent/ carer must sign too.

'I agree to abide by all of the above conditions stated in the <u>Student IT Network Acceptable Use Policy.</u>'

Name (BLOCK CAPITALS): ___________________ Year Group:___________

Student Signature: ___________________________

Parent/Carer Signature: _______________________ Date: ________________

<u>RATIFICATION DATE AND CHAIR'S SIGNATURE</u>

Ratified/Signature:

Print Name: Date: