Online Safety Policy

Policy Monitoring, Evaluation and Review

Version:	V0.3
Date created:	23.06.16
Author:	Jeff Howsin
Ratified by:	Board / Executive Team
Date ratified:	24.01.17
Review date:	Sept 18

Revision History:

Version	Date	Author	Summary of Changes:
V0.1	23.06.16	JH	New policy
V0.2	30.05.18	CM	Update to section 6
V0.3	04.09.18	CM	Update to TMET

ONLINE SAFETY POLICY

This policy will be personalised and adopted for use by the TMET Academies and is linked to the Acceptable User Policy (see Appendix 1 for AUP's linked to Key Stages as well as Staff and Parents), Online Safety resources (see Appendix 2) and Online Infringements and Sanctions (see Appendix 3).

The online safety policy is linked to other policies, e.g. Safeguarding and Child Protection policy, Anti-Bullying policy, PSHE, Computing policy and Social Media policy.

Contents

ONLINE SAFETY POLICY

1. Introduction and Overview

The purpose of this policy is to:

- Set out the key principles expected of all members of the academy community with respect to the use of IT-based technologies.
- Safeguard and protect the children and staff.
- Assist academy staff working with children to work safely and responsibly with the Internet and other IT and 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 for the whole academy community.
- Have clear structures to deal with online abuse such as online bullying [noting that these need to be cross referenced with other academy policies].
- 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.

The main areas of risk for our academy community can be summarised as follows:

Content

- Exposure to inappropriate content
- Lifestyle websites promoting harmful behaviours
- Hate content
- Content validation: how to check authenticity and accuracy of online content

Contact

- Grooming (sexual exploitation, radicalisation etc.)
- Online bullying in all forms
- Social or commercial identity theft, including passwords

Conduct

- Aggressive behaviours (bullying)
- Privacy issues, including disclosure of personal information
- Digital footprint and online reputation
- Health and well-being (amount of time spent online, gambling, body image)
- Sexting
- Copyright (little care or consideration for intellectual property and ownership)

1.1. Scope

This policy applies to all members of Knighton Fields Primary Academy community (including staff, pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of academy IT systems, both in and out of the Knighton Fields Primary Academy.

1.2. Roles and Responsibilities

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 academy safeguarding. • To take overall responsibility for online safety provision; • To take overall responsibility for data management and information security (SIRO) ensuring academy's relevant Local Safeguarding Children Board (LSCB) guidance • To ensure the academy uses appropriate IT systems and services including, filtered Internet Service; • 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 receive regular monitoring reports from the Online Safety Co-coordinator; • 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 academy's arrangements for online safety; • To ensure academy website includes relevant information.

Online Safety Coordinator/ Designated Child Protection Lead (This may be the same person)	• Take day to day responsibility for online safety issues and a leading role in establishing and reviewing the academy's safety policy/documents • Promote an awareness and commitment to online safety throughout the academy community; • Ensure that online safety education is embedded within the curriculum; • Liaise with academy technical staff where appropriate; • To communicate regularly with SLT and the designated online safety governor/committee to discuss current issues, review incident logs and filtering/change control logs; • 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 / 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/Safeguarding governor (including online safety)	• To ensure that the academy has in place policies and practices to keep the children and staff safe online; • To approve the Online Safety Policy and review the effectiveness of the policy; • To support the academy in encouraging parents and the wider community to become engaged in online safety activities; • The role of the online safety Governor will include: regular review with the online safety coordinator.
Computing Curriculum Leader	• To oversee the delivery of the online safety element of the Computing curriculum.

Network Manager/technician	• To report online safety related issues that come to their attention, to the Online Safety Coordinator; • To manage the academy network and make sure that: - academy password policy is strictly adhered to and reset termly for all users - 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 academy-owned devices; - the academy's policy on web filtering is applied and updated on a regular basis. • That they keep up to date with the academy'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 academy technology and online platforms are regularly monitored and that any misuse/attempted is reported to the online safety coordinator/Principal; • To ensure appropriate backup procedures and disaster recovery plans are in place; • To keep up-to-date documentation of the academy disaster recovery plans
Data and Information (Asset Owners) Managers (IAOs)	• 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; • The academy must be registered with Information Commissioner.
Teachers	• To embed online safety in the curriculum; • To supervise and guide students carefully when engaged in learning activities involving online technology (including, extra-curricular and extended academy 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.

All staff, volunteers and contractors.	• To read, understand, sign and adhere to the academy staff Acceptable Use Agreement/Policy, and understand any updates annually. The AUP is signed by new staff on induction; • To report any suspected misuse or problem to the online safety coordinator; • 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. • Exit strategy • At the end of the period of employment/volunteering to return any equipment or devices loaned by the academy. This will include leaving PIN numbers, IDs and passwords to allow devices to be reset, or meeting with line manager and technician on the last day to log in and allow a factory reset.
Pupils	• Read, understand, sign and adhere to the Student Acceptable Use Policy annually; • 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 understand the importance of adopting safe behaviours and good online safety practice when using digital technologies out of the academy • To have the opportunity to become Digital Leaders.
Parents/carers	• To read, understand and promote the academy's Student Acceptable Use Agreement with their child/children; • To consult with the academy if they have any concerns about their children's use of technology; • To support the academy in promoting online safety and endorse the Parents' Acceptable Use Agreement which includes the students' use of the Internet and the academy's use of photographic and video images.
External groups including Parent groups	• Any external individual/organisation will sign an Acceptable Use agreement prior to using technology or the Internet within the academy; • To support the academy in promoting online safety; • To model safe, responsible and positive behaviours in their own use of technology.

1.3. Communication:

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

- Policy to be posted on the academy website/ staffroom/ classrooms.
- Policy to be part of academy induction pack for new staff.
- Regular updates and training on online safety for all staff.
- Acceptable use agreements discussed with staff and students at the start of each year. Acceptable use agreements to be issued to whole academy community, on entry to the academy.

1.4. Handling Incidents:

- The academy will take all reasonable precautions to ensure online safety.
- Staff and students are given information about infringements in use and possible sanctions.
- Online Safety Co-coordinator acts as first point of contact for any incident.
- Any suspected online risk or infringement is reported to Online Safety Coordinator that day.
- Any concern about staff misuse is always referred directly to the Principal, unless the concern is about the Principal in which case the compliant is referred to the Chair of Governors.

(See Appendix 3 - Online Safety Infringements and Sanctions)

2. Education and Curriculum

2.1. Student online safety curriculum

This academy:

- Has a clear, progressive online safety education programme as part of the Computing curriculum/PSHE and other curriculum areas as relevant. This covers a range of skills and behaviours appropriate to their age and experience;
- 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 the student Acceptable Use Agreement(s);
- Ensures staff are aware of their responsibility to model safe and responsible behaviour in their own use of technology, e.g. use of passwords, logging-off, use of content, research skills, copyright;
- Ensures that staff and student s understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright/intellectual property rights;
- Ensure students only use academy approved systems and publish within appropriately secure / age-appropriate environments.

2.2. Staff and governor training

This academy:

- Makes regular training available to staff on online safety issues and the academy's online safety education program;
- Provides, as part of the induction process, all new staff [including those on university/college placement and work experience] with information and guidance on the Online Safety Policy and the academy's Acceptable Use Agreements.

2.3. Parent awareness

This academy:

- Takes every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website / Learning Platform and information about national / local online safety campaigns / literature. Parents and carers will be encouraged to support the school / academy in promoting good online safety practice and to follow guidelines on the appropriate use of:
    - digital and video images taken at school events
    - access to parents' sections of the website / Learning Platform and on-line student / pupil records
    - their children's personal devices in the school / academy (where this is allowed)

3. Expected Conduct and Incident Management

3.1. Expected conduct

In this academy all users:

- Are responsible for using the academy IT and communication systems in accordance with the relevant Acceptable Use Agreements;
- Understand the significance of misuse or access to inappropriate materials and are aware of the consequences;
- Understand it is essential to report abuse, misuse or access to inappropriate materials and know how to do so;
- Understand the importance of adopting good online safety practice when using digital technologies in and out of the academy;
- Know and understand academy policies on the use of mobile and hand held devices including cameras.

3.2. Staff, volunteers and contractors

- Know to be vigilant in the supervision of children at all times, as far as is reasonable, and uses common-sense strategies in learning resource areas where older students have more flexible access;
- Know to take professional, reasonable precautions when working with students, previewing websites before use; using age-appropriate (student friendly) search engines where more open Internet searching is required with younger students;

3.3. Parents/Carers

- Should provide consent for students to use the Internet, as well as other technologies, as part of the online safety acceptable use agreement form;
- Should know and understand what the academy's rules of appropriate use for the whole academy community are and what sanctions result from misuse.

3.4. 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 of the academy are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the academy's escalation processes;
- Support is actively sought from other agencies as needed (e.g. UK Safer Internet Centre helpline, CEOP, Prevent Officer, Police, IWF) in dealing with online 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;
- The Police will be contacted 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 – Police, Internet Watch Foundation etc.

(See Appendix 3 - Online Safety Infringements and Sanctions)

4. Managing IT and Communication Systems

4.1. Internet access, security (virus protection) and filtering

This academy:

- informs all users that Internet/email use is monitored;
- has filtered secure broadband connectivity through RM PLC;
    - The academy broadband access will include filtering appropriate to the age and maturity of pupils either directly through broadband provider or 3rd party solutions;
    - The academy will work with the academy Broadband team to ensure that filtering procedures are continually reviewed;
    - The academy will have a clear procedure for reporting breaches of filtering. All members of the academy community (all staff and all pupils) will be aware of this procedure through acceptable use policies and training;
    - If staff or pupils discover unsuitable sites, the URL will be reported to the academy Online Safety Coordinator who will then record the incident and escalate the concern as appropriate;
    - The academy filtering system will block all sites on the Internet Watch Foundation (IWF) list;
    - Changes to the academy filtering procedures will be risk assessed by staff with educational and technical experience prior to any changes and where appropriate with consent from the Senior Leadership Team;
    - The academy Senior Leadership Team will ensure that regular checks are made to ensure that the filtering methods selected are effective;
    - Any material that the academy believes is illegal will be reported to appropriate agencies such as IWF, the Police or CEOP;
    - The academy access strategy will be designed by educators to suit the age and curriculum requirements of the pupils, with advice from network managers;
    - Changes to the filtering policies are updated by the ICT Technician (David Lovell) as directed by the Senior Leadership Team;
- ensure network health through use of suitable anti-virus software;
- Use DfE approved systems including DfE S2S, to send 'protect-level' sensitive / personal data over the Internet;
- Use encrypted devices or secure remote access where staff need to access 'protect-level' (sensitive personal) data off-site.

4.2. Network management (user access, backup)

This academy:

- Uses individual logins staff and older children. Shared logins for younger children;
- Uses guest accounts occasionally 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 local network monitoring/auditing software installed;
- Has daily back-up of academy data (admin and curriculum);
- Storage of all data within the academy will conform to the EU and UK data protection requirements; Storage of data online, will conform to the EU data protection directive where storage is hosted within the EU.

To ensure the network is used safely, this academy:

- Ensures staff read and sign that they have understood the academy's online safety Policy. Following this, they are set-up with Internet, email access and network access. Online access to service is through a unique, audited username and password;
- 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;
- Has set-up the network with a shared 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 log off when they have finished working or are leaving the computer unattended;
- Ensures all equipment owned by the academy and/or connected to the network has up to date virus protection;
- Makes clear that staff are responsible for ensuring that any computer or laptop loaned to them by the academy, is used primarily to support their professional responsibilities;
- Maintains equipment to ensure Health and Safety is followed;
- Does not allow any outside Agencies to access our network remotely except where there is a clear professional need and then access is audited restricted and is only through approved systems;
- Has a clear disaster recovery system in place that includes a secure, remote off site back up of data;
- This academy uses secure data transfer; this includes DfE secure S2S website for all CTF files sent to other academies;
- Ensures that all student level data or personal data sent over the Internet is encrypted or only sent within the approved secure system;
- Our wireless network has been secured to industry standard Enterprise security level /appropriate standards suitable for educational use;
- All IT and communications systems installed professionally and regularly reviewed to ensure they meet health and safety standards.

4.3. Password policy

This academy:

- Makes it clear that staff and students must always keep their passwords private, must not share with others; If a password is compromised the academy should be notified immediately;
- All staff have their own unique username and private passwords to access academy systems. Staff are responsible for keeping their password(s) private;
- We require staff to use STRONG passwords;
- We require staff using critical systems to use two factor authentication.
- The management of password security will be the responsibility of the Network Manager.

4.3.1. Responsibilities:

All adults 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. Pupils have access to computers via a shared class username and password.

Passwords for new users, and replacement passwords for existing users can be allocated by the ICT Technician. Any changes carried out must be notified to the member of staff responsible for issuing and coordinating password security (above).

4.3.2. Training/Awareness:

It is essential that users are made aware of the need to keep passwords secure, and the risks attached to unauthorised access/data loss. This should apply to even the youngest of users, even if class log-ons are being used.

Members of staff will be made aware of the academy's password security procedures:

- at induction;
- through the academy's Online Safety Policy and procedures;
- through the Acceptable Use Agreement;

Pupils will be made aware of the academy's password security procedures:

- in ICT and/or Online Safety lessons
- through the Acceptable Use Agreement

The following rules apply to the use of passwords:

- the last four passwords cannot be re-used;
- the password should be a minimum of 8 characters long and must include three of – uppercase character, lowercase character, number, special character;
- the account should be "locked out" following six 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);
- requests for password changes should be authenticated to ensure that the new password can only be passed to the genuine user;

The "master/administrator" passwords for the academy ICT system, used by the ICT Technician (or other person) must also be available to the Principal or other nominated senior leader and kept in a secure place (e.g. academy safe). Alternatively, where the system allows more than one "master/administrator" log-on, the Principal or other nominated senior leader should be allocated those master/administrator rights. The academy should never allow one user to have sole administrator access.

4.3.3. Audit/Monitoring/Reporting/Review:

The Senior Management Team and IT Technician will ensure that full records are kept of:

- User IDs and requests for password changes;
- User logons;
- Security incidents related to this Policy and procedures.

In the event of a serious security incident, the police may request and will be allowed access to passwords used for encryption. Local Authority Auditors also have the right of access to passwords for audit investigation purposes.

User lists, IDs and other security related information must be given the highest security classification and stored in a secure manner. These records will be reviewed at regular intervals.

4.4. E-mail

This academy:

- Provides staff with an email account for their professional use, and personal email should be through a separate account;
- Uses anonymous or group e-mail addresses, for example info@rushey-rmet.org.uk;
- Will contact the Police if one of our staff or students receives an e-mail that we consider is particularly disturbing or breaks the law;
- Will ensure that email accounts are maintained and up to date;
- We use a number of technologies to help protect users and systems in the academy;
- Staff will only use official academy provided email accounts to communicate with pupils and parents, as approved by the Senior Leadership Team;
- The forwarding of chain messages is not permitted;
- The official academy email service may be regarded as safe and secure and is monitored. Staff and pupils should therefore use only the academy email service to communicate with others when in academy, or on academy systems (e.g. by remote access);
- Users need to be aware that email communications may be monitored.

4.4.1. Emailing Personal, Sensitive, Confidential or Classified Information

- Assess whether the information can be transmitted by other secure means before using email - emailing confidential data is not recommended and should be avoided where possible;
- The use of Hotmail, BT Internet, G-mail or any other Internet based webmail service for sending email containing sensitive information is not permitted;
- Where your conclusion is that email must be used to transmit such data:
  - Obtain express consent from your manager to provide the information by email;
  - Exercise caution when sending the email and always follow these checks before releasing the email:
    - Verify the details, including accurate email address, of any intended recipient of the information;
    - Verify (by phoning) the details of a requestor before responding to email requests for information;
    - Do not copy or forward the email to any more recipients than is absolutely necessary.
  - Do not send the information to any person whose details you have been unable to separately verify (usually by phone);
  - Send the information as an encrypted document attached to an email;
  - Provide the encryption key or password by a separate contact with the recipient(s);
  - Do not identify such information in the subject line of any email;
  - Request confirmation of safe receipt.

Pupils:

- Pupils are taught about the online safety and 'netiquette' of using e-mail both in academy and at home.

Staff:

- Staff can only use the e mail systems on the academy system;
- Staff will use the e-mail systems for professional purposes;
- Access in academy to external personal email accounts may be blocked;
- Never use email to transfer staff or student personal data. 'Protect-level' data should never be transferred by email. If there is no secure file transfer solution available for the situation, then the data / file must be protected with security encryption.

4.5. Academy website

- The Principal, supported by the Governing body, takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained;
- The academy web site complies with 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;
- 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;

4.6. Cloud Environments

- Uploading of information on the academy's online learning space is shared between different staff members according to their responsibilities e.g. all class teachers upload information in their class areas;
- Photographs and videos uploaded to the academy's online environment will only be accessible by members of the academy community;
- In academy, students are only able to upload and publish within academy approved 'Cloud' systems.

4.7. Social networking

Please refer to "**Social Media Policy**"

4.7.1. Staff, Volunteers and Contractors

- 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, but to use the academy's preferred system for such communications.

4.7.2. Pupils

- 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 [age appropriate] Student Acceptable Use Agreement.

4.7.3. Parents

- Parents are reminded about social networking risks and protocols through our parental Acceptable Use Agreement and additional communications materials when required;
- Are reminded that they need to ask permission before uploading photographs, videos or any other information about other people.

4.8. CCTV

- We have CCTV in the academy as part of our site surveillance for staff and student safety. The use of CCTV is clearly signposted. We will not reveal any recordings without appropriate permission;
- 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.

4.9. Disposal of Redundant ICT Equipment

- All redundant ICT equipment will be disposed of through an authorised agency. This should include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data.
- All redundant ICT equipment that may have held personal data will have the storage media over written multiple times to ensure the data is irretrievably destroyed. Or if the storage media has failed it will be physically destroyed. We will only use authorised companies who will supply a written guarantee that this will happen.

  - Disposal of any ICT equipment will conform to:

    - The Waste Electrical and Electronic Equipment Regulations 2006
    - The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007
    - Environment Agency Guidance (WEEE) Click here to access
    - ICO Guidance - Data Protection Act 1998 Click here to access
    - Electricity at Work Regulations 1989

  - The academy will maintain a comprehensive inventory of all its ICT equipment including a record of disposal.
  - The academy's disposal record will include:

    - Date item disposed of;
    - Authorisation for disposal, including:
      - verification of software licensing
      - any personal data likely to be held on the storage media? *
    - How it was disposed of e.g. waste, gift, sale
    - Name of person and/or organisation who received the disposed item

    * if personal data is likely to be held the storage media will be over written multiple times or 'scrubbed' to ensure the data is irretrievably destroyed.

  - Any redundant ICT equipment being considered for sale/gift will have been subject to a recent electrical safety check and hold a valid PAT certificate.

5. Data Security - Management Information System access and data transfer

5.1. Strategic and operational practices

At this academy:

- The Principal is the Senior Information Risk Officer (SIRO).
- Staff are clear who are the key contact(s) for key academy information (the Information Asset Owners) are. We have listed the information and information asset owners;
- 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 a single central record.

5.2. Technical Solutions

- Staff have secure area(s) on the network to store sensitive files;
- We require staff to log-out of systems when leaving their computer, but also enforce lock-out after 10 minutes' idle time;
- All servers are in lockable locations and managed by DBS-checked staff;
- Details of all academy-owned hardware will be recorded in a hardware inventory;
- Details of all academy-owned software will be recorded in a software inventory;
- Disposal of any equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2006 and/or The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007. Further information can be found on the Environment Agency website;
- Where any protected or restricted data has been held we get a certificate of secure deletion for any server that once contained personal data;
- We are using secure file deletion software.

6. Equipment and Digital Content

6.1. Mobile Devices (Mobile phones, tablets and other mobile devices)

- Mobile devices brought into academy are entirely at the staff member, student's & parent's or visitor's own risk. The academy accepts no responsibility for the loss, theft or damage of any phone or hand held device brought into academy;
- Mobile devices are not permitted to be used in certain areas within the academy site, e.g. changing rooms and toilets.
- No images or videos should be taken on mobile devices without the prior consent of the person or people concerned;
- The recording, taking and sharing of images, video and audio on any personal mobile device is to be avoided, except where it has been explicitly agreed by the Principal. Such authorised use is to be recorded. All mobile device use is to be open to monitoring scrutiny and the Principal is able to withdraw or restrict authorisation for use at any time, if it is deemed necessary;
- The academy reserves the right to search the content of any mobile devices on the academy premises where there is a reasonable suspicion that it may contain illegal or undesirable material, including pornography, violence or bullying.

Pupils' use of personal devices

- Pupils are discouraged from bringing their mobile phones into the academy. Where it is necessary for a child to bring a phone due to the need to contact their parents before or after the academy day, the phone is handed into the academy office to be stored.
- If a student needs to contact his or her parents or carers, they will be allowed to use the academy phone. Parents are advised not to contact their child via their mobile phone during the academy day, but to contact the academy office;
- If a student breaches the academy policy, then the device will be confiscated and will be held in a secure place in the academy office. Mobile devices will be released to parents or carers in accordance with the academy policy.
- Phones and devices must not be taken into examinations. Pupils found in possession of a mobile device 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;
- 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 are not permitted to use their own mobile phones or devices in a professional capacity, such as for contacting children, young people or their families within or outside of the setting;
- Staff will have access to an academy phone where contact with students, parents or carer is required. If contact with a parent is required during an offsite visit, then a member of staff will contact the academy office for this phone call to be made.
- Mobile Phones and personally-owned devices will be switched off or switched to 'silent' mode. Bluetooth communication should be 'hidden' or switched off and mobile phones or personally-owned devices will not be used during teaching periods unless permission has been granted by a member of the senior leadership team in emergency circumstances;
- Staff should not use personally-owned devices, such as mobile phones or cameras, to take photos or videos of students unless permission has been granted by the Principal or Assistant Principal. In these circumstances, any images taken must be deleted from the mobile phone by the end of the day;
- 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 and then report the incident with the Principal / Designated Officer;
- If a member of staff breaches the academy policy then disciplinary action may be taken.
- Staff may use their phones during break times. If a staff member is expecting a personal call they may leave their phone with the academy office to answer on their behalf, or seek specific permissions to use their phone at other than their break times.

Visitor use of personal devices

- Parents/carers are advised that images of pupils, other than their own, must not be taken during assemblies and celebration events
- Contractors, visitors and volunteers are made aware upon signing in to the academy, that mobile phones should not be used where pupils are present

6.2. Storage, Synching and Access

The device is accessed with an academy owned account

- The device has an academy created account and all apps and file use is in line with this policy. No personal elements may be added to this device;
- PIN access to the device must always be known by the network manager;

The device is accessed with a personal account

- If personal accounts are used for access to an academy owned mobile device, staff must be aware that academy use will be synched to their personal cloud, and personal use may become visible in academy and in the classroom;
- PIN access to the device must always be known by the network manager;
- Exit process – when the device is returned the staff member must log in with personal ID so that the device can be Factory Reset and cleared for reuse;

6.3. Digital images and video

In this academy:

- We gain parental/carer permission for use of digital photographs or video involving their child as part of the academy agreement form when their daughter/son joins the academy;
- We do not identify students in online photographic materials or include the full names of students in the credits of any published academy produced video materials/DVDs;

- Staff sign the academy's Acceptable Use Policy and this includes a clause on the use of mobile phones/personal equipment for taking pictures of students;
- If specific student photos (not group photos) are used on the academy web site, in the prospectus or in other high profile publications the academy will obtain individual parental or student permission for its long term, high profile use;
- Students are taught about how images can be manipulated in their online safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children as part of their computing scheme of work;
- 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 risks associated with providing information with images (including the name of the file), that reveals the identity of fappendixthers and their location. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.

7. Appendices

Appendix 1 - Acceptable User Policies
Appendix 2 - Online Safety Resources
Appendix 3 - Online Infringements and Sanctions
Appendix 4 – Please refer to "Social Media Policy"

7.1. Appendix 1 - Acceptable User Policy (KS1)

KS1 Pupil Acceptable Use Agreement

Think before you click	
S	I will only use the Internet and email with an adult
A	I will only click on icons and links when I know they are safe
F	I will only send friendly and polite messages
E	If I see something I don't like on a screen, I will always tell an adult

My Name:

My Signature:

Appendix 1 - Acceptable User Policy (KS2)

KS2 Pupil Acceptable Use Agreement

These rules will keep me safe and help me to be fair to others.

- I will only use the academy's computers for academy work and homework.
- I will only edit or delete my own files and not look at, or change, other people's files without their permission.
- I will keep my logins and passwords secret.
- I will not bring files into academy without permission or upload inappropriate material to my workspace.
- I am aware that some websites and social networks have age restrictions and I should respect this.
- I will not attempt to visit Internet sites that I know to be banned by the academy.
- I will only e-mail people I know, or a responsible adult has approved.
- The messages I send, or information I upload, will always be polite and sensible.
- I will not open an attachment, or download a file, unless I know and trust the person who has sent it.
- I will not give my home address, phone number, send a photograph or video, or give any other personal information that could be used to identify me, my family or my friends, unless a trusted adult has given permission. I will never arrange to meet someone I have only ever previously met on the Internet, unless my parent/carer has given me permission and I take a responsible adult with me.
- If I see anything I am unhappy with or I receive a message I do not like, I will not respond to it but I will show a teacher / responsible adult.

I have read and understand these rules and agree to them.

Signed: *Date:*

Appendix 1 - Acceptable User Policy (KS3 and KS4)

KS3 and KS4 Pupil Acceptable Use Agreement

These rules will keep everyone safe and help us to be fair to others.

1. I will only use the academy's computers for appropriate academy activities and learning and am aware that the academy can monitor my internet use.

2. I will not bring files into the academy that can harm the academy network or be used to circumvent academy security tools.

3. I will only edit or delete my own files and not view, or change, other people's files or user areas without their permission.

4. I will keep my logins, IDs and passwords secret and change my password regularly.

5. I will use the Internet responsibly and will not visit web sites that are inappropriate for the academy or my key stage.

6. I will only e-mail or contact people I know, or those approved as part of learning activities.

7. The messages I send, or information I upload, will always be polite and sensible. All messages I send reflect on me and the academy.

8. I will be careful when opening files and attachments, checking for viruses etc. If I am unsure I will never open a file.

9. I will not give my personal information that could be used to identify me, my family or my friends on any online space, unless a trusted adult has given permission or reviewed the site.

10. I will never arrange to meet someone I have only ever previously met on the Internet or by email or in a chat room, unless I take a trusted adult with me.

11. If I see anything I am unhappy with or I receive a message that makes me feel uncomfortable, I will not respond to it but I will save it and talk to a trusted adult.

12. I am aware that some websites, games and social networks have age restrictions and I should respect this.

13. I am aware that my online activity at all times should not upset or hurt other people and that I should not put myself at risk.

I have read and understand these rules and agree to them.

Signed: *Date:*

Appendix 1 - Acceptable User Policy (Parent)

Parent Acceptable Use Agreement

Internet and ICT: As the parent or legal guardian of the pupil(s) named below, I grant permission for the academy to give my *daughter / son* access to:

- the internet at the academy;
- the academy's chosen email system;
- the academy's online learning environments;
- ICT facilities and equipment at the academy.

I accept that ultimately the academy cannot be held responsible for the nature and content of materials accessed through the Internet and mobile technologies, but I understand that the academy takes every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials.

I understand that the academy can, if necessary, check my child's computer files and the Internet sites they visit at academy and if there are concerns about my child's e-safety or e-behaviour they will contact me.

Use of digital images, photography and video: I understand the academy has a clear policy on "The use of digital images and video" (see below) and I support this.

I understand that the academy will necessarily use photographs of my child or including them in video material to support learning activities.

I accept that the academy may use photographs / video that includes my child in publicity that reasonably promotes the work of the academy, and for no other purpose.

I will not take and then share online, photographs of other children (or staff) at academy events without permission.

Social networking and media sites: I understand that the academy has a clear policy on "The use of social networking and media sites" (see below) and I support this.

I understand that the academy takes any inappropriate behaviour seriously and will respond to observed or reported inappropriate or unsafe behaviour.

I will support the academy by promoting safe use of the Internet and digital technology at home. I will inform the academy if I have any concerns.

My daughter / son name(s): _____

Parent / guardian signature: _____

Date: ___/___/___

The use of digital images and video

To comply with the Data Protection Act 1998, we need your permission before we can photograph or make recordings of your daughter / son.

We follow the following rules for any external use of digital images:

If the pupil is named, we avoid using their photograph.

If their photograph is used, we avoid using the pupils' full name.

Where showcasing examples of pupils work we only use their first names, rather than their full names.

If showcasing digital video work to an external audience, we take care to ensure that pupils aren't referred to by name on the video, and that pupils' full names aren't given in credits at the end of the film.

Only images of pupils in suitable dress are used.

Staffs are not allowed to take photographs or videos on their personal equipment.

Examples of how digital photography and video may be used at the academy include:

- Your child being photographed (by the class teacher or teaching assistant) as part of a learning activity;
  e.g. taking photos or a video of progress made by a nursery child, as part of the learning record, and then sharing with their parent / guardian.

- Your child's image being used for presentation purposes around the academy;
  e.g. in class or wider academy wall displays or PowerPoint© presentations.

- Your child's image being used in a presentation about the academy and its work in order to share its good practice and celebrate its achievements, which is shown to other parents, academies or educators;
  e.g. within a CDROM / DVD or a document sharing good practice; in our academy prospectus or on our academy website.
  In rare events, your child's picture could appear in the media if a newspaper photographer or television film crew attends an event.

Note: If we, or you, actually wanted your child's image linked to their name we would contact you separately for permission, e.g. if your child won a national competition and wanted to be named in local or government literature.

The use of social networking and on-line media

This academy asks its whole community to promote the 3 commons approach to online behaviour:

- **Common courtesy**
- **Common decency**
- **Common sense**

How do we show common courtesy online?

- We ask someone's permission before uploading photographs, videos or any other information about them online.
- We do not write or upload 'off-hand', hurtful, rude or derogatory comments and materials. To do is disrespectful and may upset, distress, bully or harass.

How do we show common decency online?

- We do not post comments that can be considered as being **intimidating, racist, sexist, homophobic or defamatory. This is cyber-bullying** and may be harassment or libel.
- When such comments exist online, we do not forward such emails, tweets, videos, etc. By creating or forwarding such materials we are all liable under the law.

How do we show common sense online?

- We think before we click.
- We think before we upload comments, photographs and videos.
- We think before we download or forward any materials.
- We think carefully about what information we share with others online, and we check where it is saved and check our privacy settings.
- We make sure we understand changes in use of any web sites we use.
- We block harassing communications and report any abuse.

Any actions online that impact on the academy and can potentially lower the academy's (or someone in the academy) reputation in some way or are deemed as being inappropriate will be responded to.

Appendix 1 - Acceptable User Policy (Staff, Volunteers and Contractors)

Staff, Volunteers and Contractors Acceptable Use Agreement

This covers use of all digital technologies in academy: i.e. email, Internet, intranet, network resources, learning platform, software, communication tools, equipment and systems.

- I will only use the academy's digital technology resources and systems for Professional purposes or for uses deemed 'reasonable' by the Principal and Governing Body.
- I will not reveal my password(s) to anyone.
- I will follow 'good practice' advice in the creation and use of my password. If my password is compromised, I will ensure I change it. I will not use anyone else's password if they reveal it to me and will advise them to change it.
- I will not allow unauthorised individuals to access email / Internet / intranet / network, or other academy systems.
- I will ensure all documents, data etc., are printed, saved, accessed and deleted / shredded in accordance with the academy's network and data security protocols.
- I will not engage in any online activity that may compromise my professional responsibilities.
- I will only use the approved email system(s) for any academy business.
- I will only use the approved communication systems with pupils or parents/carers, and only communicate with them on appropriate academy business.
- I will not browse, download or send material that is considered offensive or of an extremist nature by the academy.
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach or equipment failure to the *appropriate line manager*.
- I will not download any software or resources from the Internet that can compromise the network or might allow me to bypass the filtering and security system or are not adequately licensed.
- I will check copyright and not publish or distribute any work including images, music and videos, that is protected by copyright without seeking the author's permission.
- I will not connect any device (including USB flash drive), to the network that does not have up-to-date anti-virus software, and I will keep any 'loaned' equipment up-to-date, using the academy's *recommended anti-virus and other ICT 'defense' systems*.
- I will not use personal digital cameras or camera phones or digital devices for taking, editing and transferring images or videos of pupils or staff and will not store any such images or videos at home.
- I will follow the academy's policy on use of mobile phones / devices at academy.
- I will only use academy approved equipment for any storage, editing or transfer of digital images / videos and ensure I only save photographs and videos of children and staff on the *appropriate system or staff-only drive within the academy*.
- I will use the academy's Learning Platform in accordance with academy protocols.
- I will ensure that any private social networking sites / blogs etc. that I create or actively contribute to are not confused with my professional role.
- I will ensure, where used, I know how to use any social networking sites / tools securely, so as not to compromise my professional role.

- I agree and accept that any computer or laptop loaned to me by the academy, is provided solely to support my professional responsibilities and that I will notify the academy of any "significant personal use" as defined by HM Revenue & Customs.
- I will only access academy resources remotely (such as from home) using the academy approved system and follow e-security protocols to interact with them.
- I will ensure any confidential data that I wish to transport from one location to another is protected by encryption and that I follow academy data security protocols when using any such data at any location.
- I understand that data protection policy requires that any information seen by me with regard to staff or pupil information, held within the academy's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.
- I will alert the child protection officer / appropriate senior member of staff if I feel the behaviour of any child may be a cause for concern.
- I understand it is my duty to support a whole-academy safeguarding approach and will report any behaviour of other staff or pupils, which I believe may be inappropriate or concerning in any way, to a senior member of staff / designated Child Protection lead.
- I understand that all Internet and network traffic / usage can be logged and this information can be made available to the Principal / Safeguarding Lead on their request.
- I understand that Internet encrypted content (via the https protocol), may be scanned for security and/or safeguarding purposes.
- *If applicable, I will only use any LA system I have access to in accordance with their policies.*
- *If applicable,* I will embed the academy's on-line safety / digital literacy / counter extremism curriculum into my teaching.

User Signature

- I agree to abide by all the points above.
- I understand that I have a responsibility for my own and others e-safeguarding and I undertake to be a 'safe and responsible digital technologies user'.
- I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the academy's most recent online safety policies.
- I understand that failure to comply with this agreement could lead to disciplinary action.

Signature .....Date.....

Full Name ..... (printed)

Job title / Role .....

7.2. Appendix 2 - Online Safety Resources

Online Safety Resources

National Agencies

- Child Exploitation and Online Protection centre CEOP's homepage - report concerns to CEOP via the "Click Ceop" button
- Virtual Global Taskforce - VGT homepage
- Think U Know - Advice for Parents, Teachers and Young people and teaching resources
- Internet Watch Foundation - Report illegal Content online
- Childnet International – Guidance for Parents, Teachers, Children and Young People
- UK Safer Internet Centre
- NEN E-Safety

e-Safety Curriculum Materials

- ThinkUKnow - Material from CEOP aimed at children aged 4 to 16 (KS1/2/3/4)
- All about Explorers - Evaluate reliability of online information (KS2/3)
- Create a Buddie - Primary tool and Secondary tool (Use the Demo version to avoid registering)
- Websafecrackerz - Online activities (KS2/3)
- Welcome to the Web (KS2/3)
- Ideas to Inspire Internet Safety
- Webwise - resource from Ireland (KS2/3)
- e-Safety Games Online Games from the North West Learning Grid (KS2/3)
- Young People Safe online - Advice and Resources for Young People (KS2/3)
- The Quality Information Checklist - Useful tool to check websites (KS2/3)
- Kidsmart - Activities, Videos and information (KS1/2/3)
- ChildLine Online Safety Advice
- Information Comissoners Office - Guidance for Young People (KS3/4)
- I Keep Safe - (KS1/2/3/4)
- Netsmartz - (KS1/2/3/4)
- Get Netwise - (KS2/3/4)

For Parents

- Think U Know: Parents/carers Guide to the Internet
- Direct Gov: Internet Safety - Advice for parents
- Get Safe Online - Advice and guidance on Safety online
- Go On - Free online learning course about basic Internet skills and safety
- Digital Parenting Magazine - Advice from Industry for Parents/carers
- Disney's Online Safety
- Yahoo Safety Tips
- Google Family Safety
- Microsoft UK Safety and Security Centre
- Click CEOP Browser Safety Tools - Download the Click CEOP button onto web browsers
- Common Sense Media - American site which reviews websites, games
- BBC Webwise - Online Basics from the BBC
- BBC Webwise "Share Take Care" - Guidance for parents/carers on Social Networking
- NetLingo – Common Online acronyms and text speak e.g. LOL, POS
- Parents' Guide to Facebook

7.3. Appendix 3 - Online Safety Infringements and Sanctions

Online Safety Infringements and Sanctions

STUDENT	
Category A infringements	**Possible Sanctions:**
• Use of non-educational sites during lessons • Unauthorised use of email • Unauthorised use of mobile phone (or other new technologies) in lessons e.g. to send texts to friends • Use of unauthorised instant messaging / social networking sites	**Refer to class teacher / tutor** Escalate to: senior manager / Online-Safety Coordinator
Category B infringements	**Possible Sanctions:**
• Continued use of non-educational sites during lessons after being warned • Continued unauthorised use of email after being warned • Continued unauthorised use of mobile phone (or other new technologies) after being warned • Continued use of unauthorised instant messaging / chatrooms, social networking sites, NewsGroups • Use of File sharing software e.g. Napster, Vanbasco, BitTorrent, LiveWire, etc. • Trying to buy items over online • Accidentally corrupting or destroying others' data without notifying a member of staff of it • Accidentally accessing offensive material and not logging off or notifying a member of staff of it	**Refer to Class teacher/ Assistant Principal / Online-Safety Coordinator** Escalate to: removal of Internet access rights for a period / removal of phone until end of day / contact with parent]

STUDENT	
Category C infringements	**Possible Sanctions:**
• Deliberately corrupting or destroying someone's data, violating privacy of others or posts inappropriate messages, videos or images on a social networking site. • Sending an email or MSN message that is regarded as harassment or of a bullying nature (one-off) • Trying to access offensive or pornographic material (one-off) • Purchasing or ordering of items online • Transmission of commercial or advertising material • Continued sending of emails or MSN messages regarded as harassment or of a bullying nature after being warned • Deliberately creating accessing, downloading or disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent • Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988 • Bringing the academy name into disrepute	**Refer to Class teacher / Assistant Principal / Principal / removal of Internet and/or Learning Platform access rights for a period** Escalate to: contact with parents / removal of equipment **Other safeguarding actions** **if inappropriate web material is accessed:** Ensure appropriate technical support filters the site **Refer to Principal / Contact with parents** **Other possible safeguarding actions:** • Secure and preserve any evidence • Inform the sender's e-mail service provider. • Liaise with relevant service providers/ instigators of the offending material to remove Report to Police / CEOP where child abuse or illegal activity is suspected

(How will infringements be handled? If the Online-Safety Policy has been infringed, the final decision on the sanction is with the academy's senior management.)

STAFF	
Category A infringements (Misconduct)	**Possible Sanctions:**
• Excessive use of Internet for personal activities not related to professional development e.g. online shopping, personal email, instant messaging etc. • Use of personal data storage media (e.g. USB memory sticks) without considering access and appropriateness of any files stored. • Not implementing appropriate safeguarding procedures. • Any behaviour on the World Wide Web that compromises the staff members professional standing in the academy and community. • Misuse of first level data security, e.g. wrongful use of passwords. • Breaching copyright or license e.g. installing unlicensed software on network.	**Referred to line manager / Principal** Escalate to: *Warning given*

Category B infringements (Gross Misconduct)	Possible Sanctions:
• Serious misuse of, or deliberate damage to, any academy / Council computer hardware or software; • Any deliberate attempt to breach data protection or computer security rules; • Deliberately creating, accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent; • Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988; • Bringing the academy name into disrepute	**Referred to Principal / Governors**; • Other safeguarding actions: • Remove the PC to a secure place to ensure that there is no further access to the PC or laptop. • Instigate an audit of all ICT equipment by an outside agency, such as the academy's ICT managed service providers - to ensure there is no risk of pupils accessing inappropriate materials in the academy. • Identify the precise details of the material. • Escalate to: • report to LA /LSCB, Personnel, Human resource. • Report to Police / CEOP where child abuse or illegal activity is suspected. ,

If a member of staff commits an exceptionally serious act of gross misconduct

The member of staff should be instantly suspended. Normally though, there will be an investigation before disciplinary action is taken for any alleged offence. As part of that the member of staff will be asked to explain their actions and these will be considered before any disciplinary action is taken.

The academy are likely to involve external support agencies as part of these investigations e.g. an ICT technical support service to investigate equipment and data evidence, the Local Authority Human Resources team.

Child abuse images found

In the case of Child abuse images being found, the member of staff should be **immediately suspended** and the Police should be called.

Anyone may report any inappropriate or potentially illegal activity or abuse with or towards a child online to the Child Exploitation and Online Protection (CEOP):

http://www.ceop.gov.uk/reporting_abuse.html

How will staff and students be informed of these procedures?

- They will be fully explained and included within the academy's online-safety acceptable use agreement form;
- Pupils will be taught about responsible and acceptable use and given strategies to deal with incidents so they can develop unacceptable behaviours'.
- Pupils will sign an age appropriate online-safety / acceptable use agreement form;
- The academy's online-safety policy will be made available and explained to parents, and parents will sign an acceptance form when their child starts at the academy.

  Information on reporting abuse / bullying etc. will be made available by the academy for pupils,