



St Nicholas CE Primary Academy

Online Safety Procedure

April 2022



Infinity Academies Trust

Ready to learn; Prepared to flourish.

Contents

1. Introduction and Overview (Pg 3-8)

- Rationale and Scope
- Roles and responsibilities
- How the procedure is communicated to staff/pupils/community
- Handling complaints
- Reviewing and Monitoring

2. Education and Curriculum (Pg 9-10)

- Pupil online safety curriculum
- Staff and governor training
- Parent awareness and training

3. Expected Conduct and Incident Management (Pg 11-12)

4. Managing the IT Infrastructure (Pg 13-15)

- Internet access, security (virus protection) and filtering
- Network management (user access, backup, curriculum and admin)
- Passwords procedure
- E-mail
- Academy website
- Social networking

5. Data Security (Pg 16)

- Management Information System access
- Data transfer

6. Equipment and Digital Content (Pg 17-19)

- Personal mobile phones and devices
- Digital images and video

Appendices: (Pg 20-22)

A1: Acceptable Use Agreement (Staff, Volunteers and Governors)

A2: Acceptable Use Agreements (Pupils)

Search and Confiscation guidance from DfE <https://www.gov.uk/government/publications/searching-screening-and-confiscation>

1. Introduction and Overview

Rationale

The purpose of this procedure is to:

- Safeguard children and staff by setting out the key principles expected of all members of the Academy community at St Nicholas CE Primary Academy with respect to the use of IT-based technologies.
- Assist 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 community.
- Have clear structures to deal with online abuse such as online bullying [noting that these need to be cross referenced with other Trust policies & Academy procedures].
- 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, peer on peer abuse)
- 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)

Commerce (KCSIE 2021)

- risks such as online gambling,
- inappropriate advertising,
- phishing

- financial scams.

Scope

This procedure applies to all members of the St Nicholas CE Primary Academy community (including staff & Governors, students/pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of St Nicholas IT systems, both in and out of the Infinity Academies Trust.

Roles and responsibilities

Headteacher

- 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 ensuring the Academy's provision follows best practice in information handling.
- 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 needs of pupils, including the risk of children being radicalised.
- To ensure Governors are regularly updated on the effectiveness of the Academy's arrangements for online safety.
- To ensure St Nicholas CE Primary Academy website includes relevant information.

Computing Lead and Designated Safeguarding Lead

- Take day-to-day responsibility for online safety issues and a leading role in establishing and reviewing the Academy's online safety procedure/documents.
- Promote an awareness and commitment to online safety throughout the community.
- Ensure that online safety education is embedded within the curriculum.
- Liaise with technical staff where appropriate.
- To communicate regularly with SLT and the designated online safety Governor to discuss current issues & review incident 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 pupil surveys/ pupil 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 including E-Safety

- To ensure that the Academy has in place procedures, policies and practices to keep the children and staff safe online.
- To approve the Online Safety Procedure and review the effectiveness of the procedure.
- 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 who is also the Safeguarding link Governor will include: regular review with the Computing Lead and DSL.
- To oversee the delivery of the online safety element of the computing curriculum.

Computing Lead

- To report online safety related issues that come to their attention, to the DSL.
- That they keep up to date with the Academy's online safety procedure and technical information in order to effectively carry out their online safety role and to inform and update others as relevant.
- 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 the Information Commissioner.

Teachers

- To have up to date awareness of online safety matters.
- To embed online safety in the curriculum.
- To supervise and guide pupils carefully when engaged in learning activities involving online technology (including, extra-curricular and extended Academy activities if relevant).
- To ensure that pupils 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/ Procedure, and understand any updates annually. The AUP is signed by new staff on induction.
- To report any suspected misuse or problem to the DSL.
- 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.
- 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 and adhere to the Pupil Acceptable Use Procedure 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 Academy and realise that the Academy's online safety procedure covers their actions out of the Academy.
- To contribute to any 'pupil voice'/ surveys that gather information of their online experiences.

Parents/carers

- To read, understand and promote the Academy's Pupil Acceptable Use Agreement with their child/ren.
- To consult with the Academy if they have any concerns about their child/ren's use of technology.
- To support the Academy in promoting online safety and endorse the Parents' Acceptable Use Agreement which includes the pupils' 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.

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

- Procedure to be posted on the Academy website.
- Procedure 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 pupils at the start of each year.
- Acceptable use agreements to be issued to whole community, on entry to the Academy in Admissions Pack.

Handling Complaints

- St Nicholas CE Primary Academy will take all reasonable precautions to ensure online safety.
- Staff and pupils are given information about infringements in use and possible sanctions.
- Class Teacher acts as first point of contact for any incident.
- Any suspected online risk or infringement is reported to Computing Lead that day and logged on CPOMS.
- Any concern about staff misuse is always referred directly to the Headteacher, unless the concern is about the Headteacher in which case the complaint is referred to the Chair of Academy Development Committee and the LADO (Local Authority's Designated Officer).

Handling a sexting / nude selfie incident:

UKCCIS "Sexting in Academies and Colleges" should be used. This extract gives the initial actions that should be taken:

There should always be an initial review meeting, led by the DSL. This should consider the initial evidence and aim to establish:

- Whether there is an immediate risk to a young person or young people.

When assessing the risks the following should be considered:

- Why was the imagery shared? Was the young person coerced or put under pressure to produce the imagery?
- Who has shared the imagery? Where has the imagery been shared?
- Was it shared and received with the knowledge of the pupil in the imagery?
- Are there any adults involved in the sharing of imagery?
- What is the impact on the pupils involved?
- Do the pupils involved have additional vulnerabilities?
- Does the young person understand consent?
- Has the young person taken part in this kind of activity before?
- If a referral should be made to the police and/ or children's social care.
- If it is necessary to view the imagery in order to safeguard the young person – in most cases, imagery should not be viewed.
- What further information is required to decide on the best response?
- Whether the imagery has been shared widely and via what services and/or platforms. This may be unknown.
- Whether immediate action should be taken to delete or remove images from devices or online services.
- Any relevant facts about the young people involved which would influence risk assessment.
- If there is a need to contact another Trust school, Academy, college, setting or individual.
- Whether to contact parents or carers of the pupils involved - in most cases parents should be involved.
- An immediate referral to police and/or children's social care should be made if at this initial stage:

1. The incident involves an adult.

2. There is reason to believe that a young person has been coerced, blackmailed or groomed, or if there are concerns about their capacity to consent (for example owing to special educational needs).

3. What you know about the imagery suggests the content depicts sexual acts which are unusual for the young person's developmental stage, or are violent.

4. The imagery involves sexual acts and any pupil in the imagery is under 13.

5. You have reason to believe a pupil - or pupils - is at immediate risk of harm owing to the sharing of the imagery, for example, the young person is presenting as suicidal or self-harming.

If none of the above apply, then an Academy may decide to respond to the incident without involving the police or children's social care (a Trust can choose to escalate the incident at any time if further information/ concerns come to light).

The decision to respond to the incident without involving the police or children's social care would be made in cases when the DSL is confident that they have enough information to assess the risks to pupils involved and the risks can be managed within the Academy's pastoral support and disciplinary framework and if appropriate, local network of support.

Reviewing and Monitoring Online Safety

- The online safety procedure is referenced within other Academy policies (e.g. Safeguarding and Child Protection procedure, Anti-Bullying procedure, RSHE).
- The online safety procedure will be reviewed annually or when any significant changes occur with regard to the technologies in use within the Academy.
- There is widespread ownership of the procedure and it has been agreed by the SLT and approved by Governors. All amendments to the Academy online safety procedure will be disseminated to all members of staff and pupils.

2. Education and Curriculum

Pupil online safety curriculum

This Academy:

- has a clear, progressive online safety education programme as part of the Computing and RSHE curriculum. 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 pupil 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, ViewPure;
- ensures that staff and pupils understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright/ intellectual property rights;
- ensures pupils only use Academy-approved systems and publish within appropriately secure/ age-appropriate environments;
- Key online safety messages will be reinforced through assemblies, workshops, visitors, shared information using NOS resources and RSHE activities;
- Pupils will be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making;
- Pupils should be helped to understand the need for the Pupil Acceptable Use Agreement and encouraged to adopt it.

Staff and governor training

The Academy:

- Will ensure that all staff have regular online safety training as part of the 6-year Safeguarding Training plan and will receive weekly Safeguarding Updates which will cover key online safety aspects.
- All staff, including Governors and Central Team Staff members, will have access to the National Online Safety training platform.
- 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 Procedure and the Academy's Acceptable Use Agreements.

Parent awareness and training

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

across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

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

- Curriculum activities
- Letters, newsletters, academy website
- Coffee mornings
- Parents/ Carers consultation evenings
- There is an open-door policy where parents/ carers may seek advice/ guidance on online safety issues
- High profile events/ campaigns e.g. Safer Internet Day, Safer Internet week every term
- Reference to the relevant websites/ publications e.g. swgfl.org.uk
www.saferinternet.org.uk/ <http://www.childnet.com/parents-and-carers>
www.nationalonlinesafety.com
- Assigning all parents/ carers a National Online Safety login so that child-specific learning can be assigned alongside more general help sheets and awareness posters.

3. Expected Conduct and Incident Management

Expected conduct

In this Academy, all users:

- Are responsible for using the Academy's 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 procedures on the use of mobile and hand-held devices, including cameras and smartphones.

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 pupils have more flexible access;
- Know to take professional, reasonable precautions when working with pupils, previewing websites before use; using age-appropriate (pupil friendly) search engines where more open Internet searching is required with younger pupils; use ViewPure where possible to filter unwanted/ inappropriate adverts.

Parents/Carers:

- Should provide consent for pupils 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 community' are and what sanctions result from misuse.

Incident Management

In this Academy:

- There is strict monitoring and application of the online safety procedure and a differentiated and appropriate range of sanctions are available (depending on the situation), all concerns are logged using CPOMS;
- 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 (i.e. Infinity Academies Trust Central Team, the Local Authority, Safer Internet Centre helpline, CEOP, Prevent Officer, Police, PCSOs) in dealing with online safety issues;
- Monitoring and reporting of online safety incidents takes place and contributes to developments in procedure 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 pupils 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 and inform the LA.

Managing IT and Communication System

Internet access, security (virus protection) and filtering

The Academy:

- Informs all users that Internet/email use is monitored;
- Uses encrypted devices or secure remote access where staff need to access 'protect-level' (sensitive personal) data off-site;
- Uses multi-factor authentication for all staff devices;
- 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 Procedure. 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. The same credentials are used to access the Academy's network. We also provide a different/ use the same username and password for access to our Academy's network;
- All staff use multi-factor authentication in order to access the network;
- All pupils have their own unique username which gives them access to the Internet and other services;
- Makes clear that no one should log on as another user and makes clear that pupils should never be allowed to log-on, or use, teacher and staff logins;
- Has set-up the network with a shared work area for pupils and one for staff. Staff and pupils 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;
- Makes clear that staff accessing LA systems do so in accordance with any Corporate policies; e.g. Borough email or Intranet; finance system, Personnel system etc;
- Maintains equipment to ensure Health and Safety is followed;
- Ensures that access to the Academy's network resources from remote locations by staff is audited and restricted and access is only through Trust/ LA approved systems;
- 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 this is only accessed through approved systems);
- All IT and communications systems are installed professionally and are regularly reviewed to ensure they meet health and safety standards.

Password procedure

- This Academy makes it clear that staff must always keep their passwords private and must not be shared with others. If a password is compromised, the Academy should be notified immediately.
- All staff have Bit Locker installed on their laptop so that multi-factor authentication is required to gain access.
- All staff have their own unique username and private passwords to access Academy systems. Staff are responsible for keeping their password(s) private and regularly updating it.
- We require staff to use STRONG passwords.
- We require staff to change their passwords twice a year.
- We require staff to use the 'Authenticator' app for multi-factor authentication when working off-site.

E-mail

This Academy:

- Provides staff with an email account for their professional use and makes clear that personal email should be through a separate, personal account.
- Will contact the Police if one of our staff or pupils receives an e-mail that we consider is particularly disturbing, breaks the law or appears to contain links to ransomware.

Personal devices:

- May only be used during break times where staff are classroom based.
- Are to be stored away from sight.
- Under no circumstances should staff be expected or allowed to use their personal equipment to take images of pupils at, or on behalf of, the school.
- Visitors will be reminded by office staff that mobile phone use for photography is not permitted on the premises.

Pupils:

- Have access to NOS lessons, resources and guides.
- Enjoy a termly 'focus-week' where online safety is explored, highlighted and taught.
- Pupils are taught about online safety and 'netiquette' of using e-mail both in school and at home.

Staff:

- Have access to NOS lessons, resources and guides.
- Staff will use school e-mail systems for professional purposes.
- Never use email to transfer staff or pupil 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.

St Nicholas CE Primary Academy website

- The Headteacher, supported by the Governing board, takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained;
- The Academy website 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 pupils' names when saving images in the file names or in the tags when publishing to the Academy website.

Cloud Environments

- Photographs and videos uploaded to the Academy's online environment will only be accessible by members of the Academy community.

Social networking

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.

Academy staff will ensure that in private use:

- No reference should be made in social media, except via Twitter accounts, to students/pupils, parents/carers or Trust staff;
- Academy staff should not be online friends with any pupil. Any exceptions must be approved by the Headteacher;
- They do not engage in online discussion on personal matters relating to members of the Academy community;
- Personal opinions should not be attributed to the Academy or local authority and personal opinions must not compromise the professional role of the staff member, nor bring the Academy or Trust into disrepute;
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

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] pupil Acceptable Use Agreement.

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.

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

Strategic and operational practices

In this Academy:

- The Headteacher is the Senior Information Risk Officer (SIRO).
- Staff are clear who are the key contact(s) for key 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.

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.
- 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.

6. Equipment and Digital Content

Mobile Devices (Mobile phones, tablets, smart watches and other mobile devices)

- Mobile devices brought into the Academy are entirely at the staff member, students & parents or visitors' own risk. The Academy accepts no responsibility for the loss, theft or damage of any phone or hand-held device brought into the Academy.
- No student should bring his or her mobile phone or personally-owned device - including any internet enabled smart-watches - into school, unless this has been agreed by the class teacher. Any devices will be handed in to the school office. Any device brought into the Academy without prior authorisation will be confiscated and returned at the end of the school day.
- The Bluetooth (or similar function) of a mobile device should be switched off at all times and not be used to send images or files to other mobile devices or make contact with people outside of the school building.
- Staff members may use their phones during break times.
- All visitors are requested to keep their phones on silent.
- The recording, taking and sharing of images, video and audio on any personal mobile device is forbidden.
- 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.

Staff mobile devices may be searched at any time as part of

- routine monitoring.
- 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 or smart watch during the school day, but to contact the school office.
- Staff may use their phones during break times. If a staff member is expecting a personal call they may leave their phone with the school office to answer on their behalf, or seek specific permissions to use their phone at a time other than their break times.

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 procedure. No personal elements may be added to this device.
- 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 the Academy and in the classroom.
- Exit process – when the device is returned the staff member must log in with personal ID so that the device can be returned to Factory Reset and cleared for reuse.

Students' use of personal devices

- The Academy strongly advises that student mobile phones, smart watches and other portable personal devices should not be brought into the Academy.

- The Academy accepts that there may be particular circumstances in which a parent wishes their child to have a mobile phone for their own safety which should be handed to the Main Office immediately upon arrival.
- If a student is found to have breached the Academy procedure, then the device will be confiscated and will be held in a secure place in the Main Office. Mobile devices, including smart watches, will be released to parents or carers in accordance with the Academy procedure.
- 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, smart watches and personally-owned devices; they will be made aware of boundaries and consequences of misuse.

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, unless they have 'Withheld' their number.
- 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.
- 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 senior leadership team.
- Staff should not use personally-owned devices, such as mobile phones, smart watches or cameras, to take photos or videos of students and will only use work-provided equipment for this purpose.
- 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 or altering the Settings) their own mobile number for confidentiality purposes and then report the incident with the Headteacher / Designated Officer.
- If a member of staff breaches the Academy procedure then disciplinary action may be taken.

Digital images and video

In this Academy:

- We gain parental/carers permission for use of digital photographs or video involving their child as part of the Academy agreement form when their child joins the Academy (or annually);
- We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published Academy produced video materials/DVDs;
- Staff sign the Academies Acceptable Use Procedure and this includes a clause on the use of mobile phones/smart watches/ personal equipment for taking pictures of pupils;
- If specific pupil photos (not group photos) are used on the Academy website, in the prospectus or in other high-profile publications, the Academy will obtain individual parental or pupil permission for its long term, high profile use.

- The Academy blocks/filters access to social networking sites unless there is a specific approved educational purpose;
- Pupils 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;
- Pupils 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.
- Pupils are taught that they should not post images or videos of others without their permission.
- Pupils are taught about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location.
- Pupils are taught about the need to keep their data secure and what to do if they are subject to bullying or abuse.

Acceptable Use Procedure for Pupils and Parents

I understand that using the computer network is a privilege, which could be taken away from me.

When using academy devices I will:

- Always behave sensibly, respecting other members of our academy.
- Only log-in using my own username.
- Keep my password secret, if I have one.
- Never access or distribute any material on the network which may be considered offensive by others.
- Close down any offensive material which has been accessed by mistake and report it to my teacher.
- Be polite at all times, both to those around me and those I contact through the network.
- Report any offensive messages I receive through the network to my teacher or Headteacher.
- Not engage in playing non-educational games.
- Not download any games or other programmes without the permission of my teacher.
- Never enter my address, telephone number, photograph or any other details about me or anyone else.
- Only enter the school address after I have got permission from my teacher, and will never enter the school telephone number.
- Only use my smart watch for telling the time, not for internet use.

If I break any of these promises I will report it to my teacher as soon as possible and realise that there may be sanctions/ consequences for my actions, but that honesty will be recognised.

Pupil

As an academy user of the Internet, I agree to comply with the school rules on its use. I will use the network in a responsible way and observe all the restrictions explained to me by my academy.

Pupil's Signature **Date**

Parent/Guardian

As the parent or legal guardian of the pupil signing above, I grant permission for my child to use electronic mail and the Internet. I understand that pupils will be held accountable for their own actions. I also understand that some material on the Internet may be objectionable and I accept responsibility for setting standards for my child to follow when selecting, sharing and exploring information and media.

Parent's/Carer's Signature **Date**

Pupil's Name **Date** **Class**

Appendix 2

Staff Information Systems Code of Conduct

To ensure that staff are fully aware of their professional responsibilities when using information systems, they are asked to sign this code of conduct.

- The information systems are academy property and I understand that it is a criminal offence to use a computer for a purpose not permitted by its owner.
- I will ensure that the laptop/iPad or any technology, including all leads and cases etc, I use will be covered on my contents insurance for my home and car. If it is lost or stolen whilst in my possession and is not covered by my insurance, I will be liable for its replacement.
- I will ensure that my information systems use will always be compatible with my professional role.
- I understand that academy information systems, including social networking sites, may not be used for private purposes in work time or in any way that goes against the Teachers' Standards or in keeping with my professional role.
- I understand that it would be unprofessional to make negative or inappropriate comments concerning members of the Trust/ academy community or the management of the academy in a public arena.
- I understand that the academy may monitor my information systems and Internet use to ensure procedure compliance.
- I understand that files created for educational purposes should not be deleted without the permission of the head teacher.
- I will respect system security and I will not disclose any password or security information to anyone other than an appropriate system manager.
- I will respect confidentiality and not open or delete other people's files without their express permission.
- I will not install any software or hardware without permission.
- I will ensure that personal data is kept secure and is used appropriately, whether on-site at the academy, taken off the academy premises or accessed remotely.
- I will respect copyright and intellectual property rights.
- I will report any incidents of concern regarding children's safety to the Head Teacher or any Designated Child Protection Lead/ Deputy Designated Child Protection Leader.
- I will ensure that any electronic communications with pupils are compatible with my professional role.
- I will promote e-safety with pupils in my care and will help them to develop a responsible attitude to system use and to the content they access or create.
- I will return my laptop/iPad, leads and cases etc. to the academy in good order at the termination of my employment.

- I will not use any personal devices to take photographs or videos of pupils

The Academy may exercise its right to monitor the use of the academy's information systems, including Internet access, the interception of e-mail and the deletion of 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.

I have read, understood and agree with the Information Systems Code of Conduct.

Signed: Name:

Date: