Colwich CE Primary School
St Andrew's CE Primary School
St Peter's CE Primary School

Online Safety and the use of Technology Policy

N.B. This policy applies to all schools within the Mid-Trent MAT; text in green type is local to individual Trust schools.

Approved by MAT Board: Spring 2020

Next Review: Spring 2022

Contents

1. Online Safety and E-Learning Policy

Aims

In schools within the Mid-Trent Multi Academy Trust (hereafter called The Trust), we acknowledge the importance of using technology in the education and wider learning of our children. We consider it a priority to ensure that children are taught to use such technology safely and to encourage them to be responsible members of the online community.

Online Safety encompasses internet technologies and electronic communications such as mobile phones, as well as collaboration tools and personal publishing. It highlights the need to educate pupils, staff, parents and governors about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

End-to-End Online Safety

Online Safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and pupils, encouraged by education and made explicit through published policies.
- Sound implementation of online safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband from the Trust provider including the effective management of Web filtering and monitoring.

Teaching and learning

Why are new technologies and Internet use important?

The internet is an essential element in 21st century life for education, business and social interaction. The Trust has a duty to provide pupils with quality internet access as part of their learning experience

- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

Internet use will enhance learning

- Trust schools' internet access will be designed expressly for pupil use and will include filtering and monitoring appropriate to the age of pupils.
- Pupils will be taught what internet use is acceptable and what is not and will be given clear objectives for internet use.
- Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of pupils.
- Staff should guide pupils in online activities that will support the learning outcomes planned for the pupils' age and maturity.
- Pupils will be educated in the effective use of the Internet in research, including the skills of effective knowledge location, retrieval and evaluation.

Pupils will be taught how to evaluate internet content

- Trust schools will ensure that the copying and subsequent use of internet derived materials by staff and pupils complies with copyright law.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Trust schools' Online Safety co-ordinators will research new trends in apps, websites and content and liaise with the Digital Leaders to ensure they are covered in the teaching of Online Safety in classes.

Pupils will be taught how to stay safe online

- Curriculum planning (see section 8) will include age appropriate opportunities to discuss, role play and learn about the benefits and risks offered by online technologies, such as e-mail, mobile phones and social networking sites.
- Online Safety delivery will be mapped across the curriculum to ensure full coverage.
- Annual Online Safety surveys will highlight trends in usage of technologies by children and pick up any dangerous behaviour.

Managing Internet Access

Monitoring access

- Monitoring software is used to ensure children are safe from threats to their safety, including terrorist and extremist material, when accessing the internet in Trust schools.
- Weekly reports are generated and scrutinised by the IT coordinator. Any concerns are investigated using screen grabs from the flagged device. Records of words investigated are kept and any serious incidents are reported to the Headteacher.
- In the event that a child is found to have inputted inappropriate content or visited potentially unsafe sites, the child/children discuss this with the IT co-ordinator. The Headteacher and parents, if necessary, are informed. Any issues are then logged on an Online Safety Concern Form and consequences are run in-line with the Trust Behaviour policy for serious issues.
- Word banks containing reference to the following are flagged and reported:
  Racism and violence
  Suicide and health
  Drugs and addiction
  Acronyms and general slang
  Predators and strangers
  Swear words and profanities
  Sex words and slang
  Pornographic content
  Extremist views
  Sexual health and biology
- In recording the concerns, a short explanation of context is given to explain the presence of inappropriate content where the child is not responsible for this. This information is then communicated to the designated School Local Governor for Online Safety.
- Updates to the monitoring software are completed, where possible, to ensure the most up to date versions are used. Working with Trust schools' ICT Technicians and the forensic software provider, the IT co-ordinator will work to establish the most complete coverage of monitoring possible, including with emerging technologies.
- If staff or pupils discover an unsuitable site, the URL must be reported to the IT Coordinator.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Information system security

- Virus protection will be updated regularly on all networked computers.
- Trust schools' ICT systems capacity and security will be reviewed regularly.
- Filtering requests will be monitored and logged, with any teachers being made aware of inappropriate searches involving their class/Key Stage.

E-mail

- Pupils may only use e-mail accounts contained within 'Purple Mash' on the Trust school systems.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.

Public web published content and Trust school websites

- The contact details on Trust school websites should be the school addresses, e-mail and telephone numbers. Staff or pupils' personal information will not be published.
- E-mail addresses will be published carefully, to avoid spam harvesting.

- Trust school headteachers or nominees will take overall editorial responsibility and ensure that website content is accurate and appropriate.

Web publishing pupils' images and work

- Images published to the web will only include pupils for whom parental permission has been given.
- Pupils' full names will not be used anywhere on Trust school websites, particularly in association with photographs.
- Written permission from parents or carers will be obtained before images of pupils are electronically published to the web.
- Pupils' work will only be published to the website with the permission of the pupil.

Social networking, video messaging and personal publishing

- The blocking software company/Trust school will block/filter access to social networking sites, except those specifically purposed to support educationally approved practice.
- Staff and pupils will be advised never to give out personal details of any kind which may identify them or their location.
- Staff and pupils will be advised not to publish specific and detailed private thoughts on social networking sites or blogs (See Section 3).
- Staff and pupils will be advised against video messaging and use of video messaging in Trust schools will be banned unless required as part of a specific lesson (e.g.- Speaking to link schools abroad).
- Apps including video and image sharing (e.g. Snapchat, Tik Tok, Live.ly) will be included in Online Safety lessons and children will be told of the dangers of these.

Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out and protocols established before use in Trust schools is allowed.
- Mobile phones will not be used during lessons or formal school time, unless specifically allowed to support learning as identified by the teacher. The sending of abusive or inappropriate text messages is forbidden. (See Section 4)

Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the General Data Protection Regulations (GDPR) (2018).

Policy Decisions

Authorising internet access

- Trust schools will maintain a current record of all staff and pupils who are granted access to the school's electronic communications, which includes internet access. The record will be kept up-to-date, for instance a member of staff may leave or a pupil's access be withdrawn.
- All staff must read and sign the 'Staff Acceptable Use Policy' before using any Trust school ICT resource. (see Section 6)
- At Key Stage 1 access to the internet will be by adult demonstration or by directly supervised access to specific, approved online materials.
- Parents will be asked to sign and return a 'Parent Acceptable Use Policy' (see Section 7).
- Sanctions for inappropriate use will be drawn up and shared with staff and pupils.

Assessing risks

- Trust schools will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of internet content, it is not possible to guarantee that unsuitable material will never appear on a Trust school computer. Neither the Trust Board nor an individual school Local Governing Body can accept liability for the material accessed, or any consequences of internet access.
- Trust schools will audit ICT provision to establish if the online safety policy is adequate and that the implementation of the online safety policy is appropriate.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.
- Methods to identify, assess and minimise risks will be reviewed regularly.

Handling online safety complaints

- Complaints of internet misuse (by pupils) will be dealt with by a senior member of staff.
- Online safety issues which raise a safeguarding alarm are recorded following safeguarding protocol. Details of the incident are included, along with any follow up actions that have taken place. These incidents are to be logged under the following categories: Cyberbullying, Inappropriate Materials, Sexual Behaviour, Stranger Contact, Unsafe Behaviour.
- In the event of a member of staff reporting an online safety incident, they are to document this in writing with a member of the Senior Leadership Team.
- Pupils and parents will be informed of the complaints procedure.
- Parents and pupils should work in partnership with staff to resolve issues.
- Actions/sanctions for internet misuse by pupils will include:
    - interview/counselling by the class teacher;
    - informing parents or carers;
    - removal or restriction of internet or computer access for a period.
- Any complaint about internet misuse by staff must be referred to the relevant Trust school headteacher.
- Any complaint about internet misuse by the headteacher must be referred to the relevant Chair of the Local Governing Body in the first instance.
- The Trust's Staff Discipline policy and Staff Code of Conduct should be referred to in the case of staff misuse of the internet.

Cyberbullying – Understanding and addressing the issues

While cyberbullying is likely to be low level in primary schools, the age of pupils making proficient use of technology is ever decreasing. Therefore, the opportunities for pupils to bully or be bullied via technology, such as e-mail, texts or social networking sites, are becoming more frequent.

As such, teaching pupils about appropriate behaviours when using technology provides a vital grounding for future use. Whilst not wanting to provoke unrecognised opportunities in pupils, consideration must be given to suitable teaching and procedures to address any issues of cyberbullying.

As felt appropriate for the age and use of technology by the pupils:

- The Trust's Anti-Bullying policy and/or Behaviour policy will address cyberbullying. Cyberbullying will also be addressed in Computing, PHSE and other relevant lessons and is brought to life through activities. As with other Trust policies, all staff and young people will be included and empowered to take part in the process.
- Pupils, parents, staff, local governors and MAT trustees will all be made aware of the consequences of cyberbullying. Young people and their parents will be made aware of pupils' rights and responsibilities in their use of new technologies, and what the sanctions are for misuse.

- In cases where incidents occur outside of the school environment, Trust schools are committed to investigate and communicate with parents involved. Trust school sanctions can also be used as a result of this behaviour.
- In the event of staff being contacted or referred to in negative or insulting posts online, parents will be required to discuss this with the Headteacher and pupils involved.
- Parents will be provided with an opportunity to find out more about cyberbullying through sessions for parents, regular guidance via Trust school newsletters and updates via other digital platforms such as Class Dojo, if applicable.

Cyberbullying - How will risks be assessed?

Trust schools will take all reasonable precautions to monitor and deal with cyberbullying, whilst pupils are in their care. However, due to the global and connected nature of new technologies, it is not possible to guarantee that inappropriate use via a Trust school computer will not occur. Neither the Trust Board nor an individual school Local Governing Body can accept liability for inappropriate use or any consequences resulting outside of school.

Trust schools will proactively engage with all pupils in preventing cyberbullying by:

- understanding and talking about cyberbullying, e.g. inappropriate use of e-mail, text messages;
- keeping existing policies and practices up-to-date with new technologies;
- ensuring easy and comfortable procedures for reporting;
- promoting the positive use of technology;
- evaluating the impact of prevention activities.
- records of any incidents of cyberbullying will be kept and will be used to help to monitor the effectiveness of the school's prevention activities. (Appendix 5)
- the use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.
- methods to identify, assess and minimise risks will be reviewed regularly.

How will cyberbullying reports/issues be handled?

- Complaints of cyberbullying (by pupils) will be dealt with by a senior member of staff.
- The school's Local Governing Body to be advised of the fact that there are current issues.
- Pupils and parents will be informed of the complaints procedure.
- Parents and pupils should work in partnership with staff to resolve issues.
- Actions/sanctions for cyberbullying by pupils will include:
    - interview/counselling by the class teacher;
    - informing parents or carers;
    - removal or restriction of Internet or computer access for a period.
- Any complaint about cyberbullying by staff must be referred to the relevant Trust school headteacher.
- Any complaint about cyberbullying by the headteacher must be referred to the relevant Chair of the Local Governing Body in the first instance.
- The Trust's Staff Discipline policy and Staff Code of Conduct should be referred to in the case of staff cyberbullying.
- Evidence of offending messages, pictures or online conversations will be kept, in order to demonstrate to others what is happening. This can be used by the Trust school, internet service provider, mobile phone company, or the Police, to investigate the cyberbullying.

Communications Policy

Introducing the online safety policy to pupils

- The Trust's online safety rules will be posted in around schools and discussed with pupils at the start of each year and as the need arises. (Section 10)
- Pupils will be informed that network and internet use will be monitored.
- Instruction in responsible and safe use should precede internet access.
- An Online Safety curriculum will be included in Computing programmes covering both school and home use.
- Posters in Trust schools will reinforce Online Safety methods

Staff and the Online Safety policy

- All staff employed by the Trust will be given the Trust Online Safety Policy and its application and importance explained.
- All Trust staff will be informed that all computer and internet use will be monitored. Discretion and professional conduct is essential.
- Staff training in safe and responsible internet use and on the Trust Online Safety Policy will be provided as required.
- Staff that manage filtering systems or monitor ICT use will be supervised by senior management and local schools' online safety governors and will have clear procedures for reporting issues.

Enlisting parents' support

- Parents' attention will be drawn to the Trust Online Safety policy in newsletters, the school prospectus, on the local school websites and through parents' sessions.
- Internet issues will be handled sensitively, and parents will be advised accordingly.
- A partnership approach with parents will be encouraged. This could include parents' evenings with demonstrations and suggestions for safe home internet use.
- Advice on filtering systems and educational and leisure activities that include responsible use of the internet will be made available to parents.

2. Policy on the Use of Photography

Introduction

Positive publicity is welcomed within Trust schools. Photographs and video clips add colour, life and interest to school activities and initiatives and help the school communities to identify and celebrate the schools' achievements. We recognise that images must be used in a responsible way, respect young people's and adults' rights of privacy and are aware of child protection issues. However, we need to balance the risk against promotion. Risks can be minimised by following the guidelines detailed in this policy.

General Data Protection Regulation (GDPR)

Photos and video images of pupils and staff are classed as personal data under the terms of the GDPR 2018. For this reason, we require the consent of either the individual concerned or in the case of pupils, their parents or legal guardians before we can display these images in the media, in publications, on websites or in public places.

Child Protection Issues

Risk occurs when individual pupils can be identified by their names alongside photographs. Therefore, we will give the Christian name of the children in photographs that are displayed within Trust school buildings. We will not provide names for any other purpose unless special parental consent has been received. Only images of children in suitable dress will be taken. Should the Trust schools learn about any inappropriateness of image use involving our pupils, we will immediately act and report it as we would for any other child protection issue.

Images taken by Trust school staff

- Personal mobile devices, including phones, must not be used in any circumstances to take photographs or make recordings of children.
- Legitimate recordings and photographs should be captured using Trust school devices, e.g. cameras or tablets.
- Trust staff should report any usage of mobile devices that causes them concern to their local Headteacher.

Images taken by adults other than school staff

Trust schools encourage parents/carers to take videos and photographs of school events. However, if any image is taken by either a parent/carer or third party with a view of publication in the press then the permission of the Headteacher must be obtained and special parental consent given. Trust schools regularly remind parents that images of children (other than their own) should not be posted online on social media etc.

When a commercial photographer/film maker is used (e.g. 'Tempest') Trust schools will:

- Provide a clear brief
- Issue identification
- Inform parents and children
- Obtain consent
- Not allow unsupervised access to children

Images taken by children

Trust schools encourage children to take photographs and videos of each other as a way of recording events. This may take place in school, on school trips or on residential visits; only school owned devices will be used. The use of cameras within school, on trips or visits is part of the pleasure and the learning in the experience. There is no reason why pupils should not be allowed to take photographs as long as anyone photographing respects the privacy of the person being photographed. This is seen as part of local schools' codes of behaviour.

Infringement of this respect of privacy is akin to bullying and will be dealt with in the same way as any other branch of school discipline.

3. Policy on Social Media

Objectives

This policy sets out the Trust's policy on social networking. Social networking activities conducted online outside work, such as blogging, involvement in social networking sites such as Facebook or Twitter and posting material, images or comments on sites such as YouTube can have a negative effect on an organisation's reputation or image. This policy has been written to set out the key principles and code of conduct that are expected of all members of Trust staff with respect to their responsibilities in connection with the use of social networking sites.

Key Principles

- Everyone within Trust schools has a responsibility to ensure that they protect the reputation of their school, and to treat colleagues and members of that school with professionalism and respect.
- It is important to protect everyone in Trust schools from allegations and misinterpretations which can arise from the use of social networking sites.
- Safeguarding children is a key responsibility of all members of Trust staff and it is essential that everyone considers this and acts responsibly if they are using social networking sites out of school. Anyone working in Trust schools, either as paid employees or volunteers, must not communicate with children via social networking.
- This policy relates to social networking outside work.

Code of Conduct: Social Networking

Under no circumstances should Trust staff make negative reference to any staff member, pupil, parent or school activity/event.

The following are also **not considered acceptable**:

- The use of any Trust school's name, logo, or any other published material without prior permission from the Headteacher. This applies to any published material including the internet or written documentation.
- The posting of any communication or images which links any Trust school to any form of illegal conduct or which may damage the reputation of that school. This includes defamatory comments.
- The disclosure of confidential or business-sensitive information or the disclosure of information or images that could compromise the security of the school.
- The posting of any images of Trust employees, children, local governors or trustees or anyone directly connected with Trust schools whilst engaged in school activities.

In addition to the above, everyone must ensure that they:

- Never 'friend' a pupil at the Trust school where they are working onto their social networking site.
- Do not make any derogatory, defamatory, rude, threatening or inappropriate comments about any Trust school, or anyone at or connected with that school.
- Use social networking sites responsibly and ensure that neither their personal nor professional reputation, nor any Trust school's reputation is compromised by inappropriate postings.

Potential and Actual Breaches of the Code of Conduct

In instances where there has been a breach of the above Code of Conduct, the following will apply:

- Use of social media will be monitored closely and any breaches of this code will be investigated. Where it is found that there has been a breach of the policy this may result in action being taken under the Trust Disciplinary policy. A breach of this policy will be considered to be a serious disciplinary offence which is also contrary to the Trust schools' ethos and principles.
- The Trust and Local Governing Bodies will take appropriate action in order to protect the Trust's reputation and that of its staff, parents, governors, children and anyone else directly linked to any Trust school.

Class Dojo

Staff must ensure that only images of children where parental consent has been granted are posted on their class story. Class Dojo is to be the only medium to report on activities within class in this manner.

Whilst every attempt has been made to cover a wide range of situations, it is recognised that this policy cannot cover all eventualities. There may be times when professional judgements are made in situations not covered by this document, or which directly contravene the standards outlined in this document.

4. Policy on Mobile Devices

Introduction and Aims

In Trust schools the welfare and well-being of our pupils are paramount. The aim of the Mobile Devices policy is to allow users to benefit from modern communication technologies, whilst promoting safe and appropriate practice through establishing clear and robust acceptable mobile user guidelines. This is achieved through balancing protection against potential misuse with the recognition that mobile phones are effective communication tools.

Early Years Foundation Stage (EYFS)
Use of mobile devices within the EYFS is included within this Trust policy.

Following the Plymouth Serious Case Review, which investigated the mis-use of mobile phones by some staff within a nursery setting, Dame Clare Tickell was asked to comment on the use of mobile phones in EYFS settings in general. Her conclusion and recommendation, which form part of her report: *The Early Years: Foundations for Life, Health and Learning* can be found as an annex to this policy.

Related Trust policies

- Safeguarding
- Staff Code of Conduct
- Social Networking Code of Practice
- Educational Visits
- Staff Discipline
- Behaviour

Use of mobile devices

Personal Mobiles – Pupils

We recognise that mobile phones are part of everyday life for many children and that they can play an important role in helping pupils to feel safe and secure. However, we also recognise that they can prove a distraction in school and can provide a means of bullying or intimidating others. Therefore:

- The phone must be handed in, switched off, to the teacher first thing in the morning and collected from them by the child at home time (the phone is left at the owner's own risk).
- Mobile phones brought to school without permission will be confiscated and returned at the end of the day.
- Where mobile phones are used in or out of Trust schools to bully or intimidate others this may be considered to be cyberbullying (see section 1 above).

Personal Mobiles - Staff:

- Staff are permitted to bring personal mobile phones to school.
- Staff may keep mobile phones with them but they should be either turned off or switched to silent mode during staff/pupil contact time. Staff may not make or receive calls during teaching/contact time. If there are extreme circumstances (e.g. acutely sick relative) the member of staff should make the headteacher aware of this and may be permitted to turn on their phone, in silent mode, in the event of having to make or to receive an **emergency** call.
- Use of mobile phones is limited to non-contact time when no children are present unless the phone is being used by a member of staff whilst off site including educational visits with children present.
- Phones must be kept out of sight (e.g. drawer, handbag, pocket) when staff are with children.
- Calls/ texts must be made/ received in private during non-contact time.
- It is also strongly advised that staff use security measures to protect access to functions of their phone.
- Staff should report any usage of mobile devices that causes them concern to the Headteacher.

- Personal mobile devices, including phones, must not be used in any circumstances to take photographs of children.

Visitors including Parents:

- It is requested that parents either turn off their mobile phones or switch them to silent mode when in the school building, school grounds or whilst accompanying children off site.
- Mobile devices can be used to take photographs in school assemblies etc, but parents are reminded these pictures are for personal use and must not be uploaded on to social networking websites without the prior consent of parents of other children who may be on the photographs.

Mobile Phones for work related purposes

The Trust recognises that mobile phones provide a useful means of communication on offsite activities. However, staff should ensure that:

- Mobile use on these occasions is appropriate and professional.
- Personal mobile phones should only be used in an emergency situation to make contact with parents during school trips. Where possible, all communications should be made via the school office/Class Dojo. If the trip take place outside office hours, it may be necessary to use personal phones in some circumstances.
- Where parents are accompanying trips, they are informed not to make contact with other parents (via calls, text, email or social networking) during the trip or use their phone to take photographs of children.

Use of Mobile Devices by Staff away from Trust School Premises

Through the course of teaching, staff will require some pieces of equipment to be removed from Trust school premises. For example, laptops, Hudls, tablets and other items can be taken home but staff should ensure that:

- Items are password protected
- Best security measures are in place (storage in car boots; not left visible in homes etc.) to reduce the chance of theft or damage.
- Devices should only be used for school related business. The use of devices for other means opens the possibility of security issues or viruses.

Volunteers, Visitors, Trustees, Local Governors and Contractors

All volunteers, visitors, trustees, local governors and contractors are expected to follow the Trust Mobile Devices policy as it relates to adults whilst on the premises. On arrival, such visitors will be informed of Trust schools' expectations around the use of mobile phones.

Annex
Use of Mobile Phones in the Early Years Foundation Stage (EYFS)

"As a result of the Plymouth Serious Case Review some have called for mobile phones to be banned in Early Years settings. Inappropriate usage of mobile phones includes instances where phone calls or texts take practitioners' attention away from supervising young children, or where camera phones are used to take images of children or support abusive practice. However, banning mobile phones would create difficulties, for example where children are taken on outings, or where a setting is based in a hall without phone facilities. It is, and should remain, the responsibility of owners, leaders and managers of Early Years settings to ensure that their setting is a safe place for children that meets the requirements of the EYFS. I would expect safeguarding policies to set out clearly how mobile phones should or should not be used in settings, reflecting the individual circumstances of individual settings, and ensuring that their usage is properly monitored. ***Therefore, I do not recommend banning mobile phones in Early Years settings.****"*

[Dame Clare Tickell; para 4.8 *The Early Years: Foundations for life, health and learning*]

5. Trust Staff Acceptable Use Policy

Trust Staff ICT Acceptable Use Statement

Staff employed by the Mid-Trent Multi Academy Trust (hereafter known as 'The Trust') should sign and have a copy of the Acceptable Use Statement. In signing, staff accept that the Trust school can monitor network and Internet use to help ensure staff and pupil safety. The Trust's Online Safety policy should be consulted for further information and clarification.

1. The information and communication technology and related systems are Trust property and I understand that it is a criminal offence to use a computer for a purpose not permitted by its owner.

2. I will ensure that my information systems use will always be compatible with my professional role.

3. I understand that my information systems may not be used for private purposes, without specific permission from the Headteacher.

4. I understand that the Trust and its schools may monitor my information systems and Internet use to ensure policy compliance.

5. I will respect system security and I will not disclose any password or security information to anyone other than an appropriate system manager.

6. I will not install any software or hardware without permission.

7. I will ensure that personal data is kept secure and is used appropriately, whether in a Trust school, taken off the school premises or accessed remotely.

8. I will respect copyright and intellectual property rights.

9. I will report any incidents of concern regarding children's safety to the Trust school Online Safety Coordinator, currently Mr Gray or the Designated Child Protection Coordinator, currently Mrs Alexander.

10. I will ensure that any electronic communications with pupils are compatible with my professional role.

11. I will promote online 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.

The Trust may exercise its right to monitor the use of its schools' information systems, including internet access, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the schools' information systems 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 Technology and Communication Acceptable Use Statement.

Signed: ……

Date: ……

Accepted for Trust school by: ……

Date: ……

6. Child Acceptable Use Policy

Trust School Online Safety Agreement

Pupil Agreement

All pupils use computer facilities, including internet access, as an essential part of learning, as required by the National Curriculum. Both pupils and their parents/carers are asked to sign to show that the Online Safety Rules have been understood and agreed.

Mid-Trent Multi Academy Trust Online Safety Rules:

1. NEVER GIVE YOUR ADDRESS OR NAME TO STRANGERS ON THE INTERNET.
2. Do not eat or drink when working on ICT equipment.
3. Personal ICT equipment should be handed to the class teacher at the beginning of the day and returned at the end of the school day.
4. Ensure that you stay in your seat to avoid tripping over wires.
5. Only access the internet for the task that you have been given
6. Usage of the computers will be monitored by the IT Coordinator using forensic software. Only school appropriate content should be viewed. The Headteacher will be made aware of any inappropriate use that is reported.
7. Carry all laptops with both hands. No more than two laptops to be carried at once.
8. Only sign on with your own log-in details unless working in a group/pair. Keep your own password safe
9. Only send emails within Purple Mash, unless prior permission is given by a teacher.
10. Social networking sites are banned in school and filters are used to block access to these sites.
11. Cyber-bullying is not tolerated and will be dealt with by Mrs Alexander and Mr Gray.

Pupil: …… Class: ……

Pupil's Agreement

- I have read and I understand the school Online Safety Rules (below)
- I will use the computer, network, iPads, internet access and other new technologies in a responsible way at all times.
- I know that network and Internet access is monitored for inappropriate use.
- I understand that this agreement also covers my use of the internet and electronic devices belonging to school.

Signed (where appropriate): …… Date: ……

7. Parent Acceptable Use Policy

For Schools within the Mid-Trent Multi Academy Trust (hereafter known as The Trust) Parent/Carer Acceptable Use Policy Agreement

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

This Acceptable Use Policy is intended to ensure:

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

The Trust and its schools will try to ensure that pupils will have good access to ICT to enhance their learning and will, in return, expect the pupils to agree to be responsible users. Children are required to agree to their own acceptable use policy when they log-in to the Trust school network, using its ICT equipment.

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

Permission Form

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

- I know that my son/daughter has received, or will receive, online safety education to help them understand the importance of safe use of ICT – both in and out of school.

- I understand that the Trust and its schools will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems.

- I also understand that the Trust and its schools cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

- I understand that my child's activity on the ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

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

Pupil Name/s: ……

Parent/Carer Name: ……

Signed: ……

Date: ……

8. Online Safety Curriculum

Online Safety Curriculum Aims

- Educate children to be responsible, competent, confident and creative users of information and communication technology.
- Encourage children who evaluate and apply information technology, including new or unfamiliar technologies, analytically to solve problems they encounter online

Stage (Online Safety Resources)	Other Resources (suggested)	Soft Skills
EYFS Digi Duck – lesson planning and resources http://www.kidrex.org/- safe search engine http://www.thinkuknow.co.uk/5_7/- CEOP education site The Adventures of Smartie the Penguin - digi duck content aimed at	***Laying the foundations for online teaching*** Learn that staying safe online is similar to staying safe in the real world. Be introduced to the basics of online searching. Explore and comment on different types of websites with the teacher, which are pupils' favourites and why? Discuss how they use the computer/tablets at home and the difference between home and school use.	• Practice turning computer on and off. • Improve mouse control. • Use of swipe for tablet • Touch screen skills
Year 1 Going Places Safely - Staying safe online ABC Searching - Simple search techniques Keep it Private - Keep personal information private My Creative Work - Having ownership of what is yours Sending Email - Communication in a digital world Think You Know resources/Hector's World	MS Word iPads Paint Purple Mash	• Typing Speed: 10 words per minute • Open a program in Windows using double click • Get onto the Internet • Log off/ shut down the computer
Year 2 Staying Safe Online - Using sites suitable for age Follow the Digital Trail - Digital Footprints – Horrible Histories - www.bbc.co.uk/cbbc/watch/p01q2pq0 Screen out the Mean - Introduction to cyberbullying Using Keywords - Efficient searching Sites I like - Rating websites	MS Office Digital Camera iPads Talking Tins Purple Mash	• Typing Speed: 10 words per minute • Log onto the computer with my username • Save my work to the school network (Year Group folder) • Delete unwanted files
Year 3 Powerful Passwords - The why behind passwords	MS Office Digital Camera iPads Scratch	• Typing Speed: 20 words per minute • Save images from the internet

My Online Community - Making connections through the internet Things for Sale - Online advertising Show Respect Online - Friends online and offline Writing Good Emails - Effective communications	Purple Mash	• Search and open a program in Windows independently • Close a program properly • Use Ctrl, alt, del to log on to the network
Stage (Online Safety Resources)	**Other Resources (suggested)**	**Soft Skills**
Year 4 Rings of Responsibility - Showing respect online and offline Private and Personal Information - Sharing your information with others The Power of Words - Cyberbullying Horrible Histories Online videos- e.g.- https://www.youtube.com/watch?v=_8oyQRabV9k The Key to Keywords - Accuracy in searches Whose is it, Anyway? - Introduction to plagiarism	MS Office Digital Cameras iPads Scratch Purple Mash	• Typing Speed: 20 words per minute • Save images from the internet • Save work using shortcut buttons • Use shortcut for cut, copy and paste • Use Ctrl, alt, del to log on to the network
Year 5 Strong Passwords - Creating secure passwords Digital Citizenship Pledge - Working together You've Won a Prize! - Introduction to Spam Horrible Histories Online videos- e.g.- https://www.youtube.com/watch?v=_8oyQRabV9k How to Cite a Site - What is a citation? Picture Perfect - Digital manipulation and the implications	MS Office Digital Cameras iPads Scratch Purple Mash	• Typing Speed: 30 words per minute What to do when an program crashes (Ctrl, alt, del) • Find a recently opened document • Use shortcuts (ctrl + z) to undo mistakes • Find a recently opened document
Year 6 Talking Safely Online - Keeping personal information private Super Digital Citizen - Working together Privacy Rules - What are secure websites? What's Cyberbullying? - What is it and how to deal with it? Jigsaw video - www.youtube.com/watch?v=_o8auwnJtqE **Alex's Willy** www.youtube.com/watch?v=sch_WMjd6go (SRE**?)** Selling Stereotypes - How the media sells ideas	MS Office Digital Cameras iPads Scratch Kodu	• Typing Speed: 30 words per minute What to do when an program crashes (Ctrl, alt, del) • Find a recently opened document • Use shortcuts (ctrl + z) to undo mistakes • Find a recently opened document

Appendix 1

St. Peter's Computing Safety Rules - KS1

1. NEVER GIVE ANY PERSONAL INFORMATION TO STRANGERS ON THE INTERNET.

2.No eating or drinking.

3. Stay in your seat.

4. Carry all laptops with both hands. No more than 1 laptop to be carried at once.

5. Only use your own log-in and never tell anyone your password.

6. No social networking in school.

7. No Cyber-bullying.




St. Peter's Computing Safety Rules - KS2

1. NEVER GIVE YOUR ADDRESS OR NAME TO STRANGERS ON THE INTERNET.
2. Do not eat or drink when working on ICT equipment.
3. Ensure that you stay in your seat to avoid tripping over wires.
4. Only access the internet for the task that you have been given.
5. Search engine terms will be reviewed by Mr Gray. Only use school-appropriate search terms.
6. Carry all laptops with both hands. No more than 2 laptops to be carried at once.
7. Only sign on with your own log-in details unless working in a pair/group. Keep your own password safe.
8. Only send emails within Purple Mash, unless permission is given by a teacher.
9. Social networking sites are banned in school and filters are used to block access to these sites.
10. Cyber-bullying is not tolerated and will be dealt with by Mr Gray & Mrs Alexander.

Appendix 2

How can you support your child in a digital world?

Establishing mobile phone rules for children can be a little tricky. After all, most parents didn't grow up owning a mobile phone so knowing what's appropriate and what isn't can be a challenge. Technology also changes so quickly that it can also be hard to keep up with the latest devices, social networking sites, and apps. Without clear guidelines, many children struggle to handle the responsibility of owning a smartphone. So it's important to establish rules that will help your child make healthy choices.

Smart Phone Rules:

The mobile phone must be left downstairs before bedtime

There really isn't a good reason why a child would need her phone during the wee hours of the morning. Children who keep their phones in their rooms at night are likely to respond to text messages or social media updates in the middle of the night and it can interfere with your child's sleep.

Although there are several reasons why children shouldn't sleep with smartphones in their bedrooms, one main reason they do is the pressure many children feel to respond to messages at all hours of the night. You can take that pressure off by establishing a rule that says phones aren't allowed in your child's room over night.

Establish a rule that clearly states what time the phone must be turned off in the evening. Then, charge the phone in a common area of the home, such as in the kitchen.

No mobile phones in bedrooms

Many children just aren't ready to handle the responsibility of having a mobile phone in their bedrooms. They may not be able to resist risky behaviour such as sexting or downloading inappropriate content.

Restricting your child from using their phone in their bedroom may seem extreme, but for some families, it can be the best way to teach appropriate mobile phone use.

No mobile phone use before school

Most children don't have much time to spare before school and texting or surfing social media can waste a lot of precious minutes. So start the day off right by saying, "No phones in the morning." If your child happens to get ready early, you might consider allowing them to use their smartphone for a few minutes as a privilege before they leave.

No mobile phones at the dinner table

Don’t allow anyone to use their phones during meals. And practise being a good role model. Don't respond to text messages or emails while you're eating. Teach your child appropriate mobile phone etiquette.

No mobile phones during family time

Stress the importance of interacting with one another in-person. Make it clear that during family activities, mobile phone use is prohibited. Whether you’re visiting with extended family or you’re playing a game of catch, discourage bad mobile phone habits, like ignoring friends to text someone who isn't present.

No mobile phone use during homework

Replying to text messages or keeping up with social media can be a huge distraction for children who are trying to study. Set limits on mobile phone use during homework time.

Create a Behaviour Contract

Once you've established clear mobile phone rules, create a behaviour contract. Include the rules and the consequences your child will experience for breaking any of the rules.

You also might include what will happen if your child loses their phone, breaks it, or incurs data overage charges.

Then, have your child review and sign the contract. That way, you'll know they are clear about your expectations and any restrictions you might impose if they violate the rules.

11. Links to Other Trust Policies

- Child Protection and Safeguarding
- Behaviour
- Anti-bullying
- Staff Discipline
- Staff Code of Conduct
- Educational Visits
- PSHEE including Sex and Relationships

12. Monitoring and Review

All staff employed by the Trust are expected to ensure this policy is implemented and to have high expectations of pupils.

This policy will be reviewed biennially – as a minimum – by Trust staff; representatives of Trust schools' Local Governing Bodies and approved by the Board of the Mid-Trent MAT.

Signed:_____ (Representative of the Mid-Trent MAT)

Date of latest policy review: 26th March 2020

Date of next review: Spring 2022