The Consortium Multi-Academy Trust
Chair of the Members and Board of Trustees: Dawn Carman-Jones
Principal/CEO: Andrew Aalders-Dunthorne
Email: principal@consortiumacademy.org **Tel**: 01379 668283 / 01379 852520

Online-Safety Policy

1. Introduction

1.1 As part of the Every Child Matters agenda set out by the government, the Education Act 2002 and the Children's Act 2004, it is the duty of school/education setting or other establishments to ensure that children and young people are protected from potential harm both within and beyond the school/education setting or other establishment environment. Therefore, the involvement of children, young people and parent/carers is also vital to the successful use of online technologies.

2. Aims

- This policy aims to explain how children are educated to be safe and responsible users, capable of making good judgements about what they see, find and use. The term 'online-safety' is used to encompass the safe use of all technologies in order to protect children from potential and known risks. To emphasise the need to educate children and about the pros and cons of using new technologies both within and outside school/education setting or other establishments.
- To provide safeguards and agreement for acceptable use to guide all users, whether staff or student, in their online experiences.
- To ensure adults are clear about procedures for misuse of any technologies both within and beyond the school/education setting or other establishment.
- To develop links with parents/carers and the wider community ensuring input into policies and procedures with continued awareness of the benefits and potential issues related to technologies.

3. Roles and Responsibilities of the School

3.1 It is the overall responsibility of the Academy Head along with the Local Governing Body to ensure that there is an overview of Online-Safety as part of the wider remit of safeguarding across the school setting with further responsibilities as follows:

- The Academy Head has designated an Online-Safety Lead to implement agreed policies, procedures, staff training, curriculum requirements and take responsibility for ensuring Online-Safety is addressed in order to establish a safe COMPUTING learning environment. All staff and students are aware of takes this role within the school.
- The Academy Head, along with the Local Governing Body will need to decide if there should be a standard disclaimer on all e-mails stating that the views expressed are not necessarily those of the school/education setting or Trust.
- Time and resources should be provided for the Online-Safety Lead and staff to be trained and update policies, where appropriate.
- The Academy Head is responsible for promoting Online-Safety across the curriculum and has an awareness of how this is being developed, linked with the school development plan.
- The Academy Head should inform the Local Governing Body about the progress of or any updates to the Online-Safety curriculum (via PSHE or Computing) and ensure Governors

know how this relates to safeguarding. At the Local Governor meetings, all governors are to be made aware of Online-Safety developments.

- The Governors **MUST** ensure Online-Safety is covered within an awareness of safeguarding and how it is being addressed within the school. It is the responsibility of Governors to ensure that all safeguarding guidance and practices are embedded.
- An Online-Safety Governor (can be the Curriculum or Safeguarding Governor) ought to challenge the school with appropriate strategies which define the roles, responsibilities for the management, implementation and safety for using computing, including:

3.2 Challenging the school about having:

- Firewalls.
- Anti-virus and anti-spyware software.
- Filters.
- Using an accredited ISP (internet Service Provider).
- Awareness of wireless technology issues.
- A clear policy on using personal devices.
- Ensure that any misuse or incident has been dealt with appropriately, according to policy and procedures, and appropriate action is taken, even to the extreme of suspending a member of staff, informing the police (via establishment's agreed protocols with the police) or involving parents/carers.

4. Local Online-Safety Lead

4.1 It is the role of the designated Online-Safety Leader to:

- Appreciate the importance of online-safety within school and to recognise that all educational establishments have a general duty of care to ensure the safety of their pupils and staff.
- Establish and maintain a safe computing learning environment within the school/education setting or other establishment.
- Ensure that filtering is set to the correct level for staff and children, in the initial set up of a network, stand-a-lone PC, staff/children laptops and the website *or ensure the technician is informed and carries out work as directed*.
- Ensure that all adults are aware of the filtering levels and why they are there to protect children and young people.
- Report issues and update the Academy Head on a regular basis.
- Liaise with the PSHE, safeguarding and computing leaders so that policies and procedures are up-to-date to take account of any emerging issues and technologies.
- Update staff training (all staff) according to new and emerging technologies so that the correct Online-Safety information can be taught or adhered to.
- Transparent monitoring of the Internet and online technologies
- Keep a log of incidents for analysis to help inform future development and safeguarding, where risks can be identified.
- Work alongside the computing Lead and technician, to ensure there is appropriate and up-to-date anti-virus software and anti-spyware on the network, stand-a-lone PCs and teacher/child laptops and that this is reviewed and updated on a regular basis.

- Ensure that staff can check for viruses on laptops, stand-a-lone PCs and memory sticks or other transferable data files to minimise issues of virus transfer.
- Ensure that unsolicited e-mails to a member of staff from other sources is minimised by filter settings on emails. Refer to the staff handbook/ website for dealing with any issues arising from indecent or pornographic/child abuse images sent/received.
- Report overuse of blanket e-mails or inappropriate tones to the Academy Head.

5. Staff or Adults

5.1 It is the responsibility of all adults within the school to:

- Ensure that they know who the Senior Designated Person for Safeguarding is within school so that any misuse or incidents can be reported which involve a child.
- Where an allegation is made against a member of staff it should be reported immediately to the Academy Head/Senior Designated Person.
- In the event of an allegation made against the Academy Head, the Chair of Governors must be informed immediately (following procedures outlined in the Whistle Blowing Policy.)
- In the event of an allegation made against the Principal/CEO, the Chair of Trustees must be informed immediately (following procedures outlined in the Whistle Blowing Policy.)
- Be familiar with the Behaviour, Anti-bullying and other relevant policies so that, in the event of misuse or an allegation, the correct procedures can be followed immediately. In the event that a procedure is unknown, they will refer to the Academy Head/Senior Designated Person immediately.
- Check the filtering levels are appropriate for their children and young people and are set at the correct level. Report any concerns to the Online-Safety Lead.
- Alert the Online-Safety Lead of any new or arising issues and risks that may need to be included within policies and procedures.
- Ensure that children and young people are protected and supported in their use of technologies so that they know how to use them in a safe and responsible manner. Children and young people should know what to do in the event of an incident.
- Be up-to-date with Online-Safety knowledge that is appropriate for the age group and reinforce through the curriculum.
- Use electronic communications in an appropriate way that does not breach the Data Protection Act 1998. Remember confidentiality and not disclose information from the network, pass on security passwords or leave a station unattended when they or another user is logged in.
- To ensure that CMAT central staff/ school office managers / staff follow the correct procedures for any data required to be taken from the school/education setting or other establishment premises.
- Report accidental access to inappropriate materials to the Online-Safety Lead in order that inappropriate sites are added to the restricted list or control this with the Local Control options via your broadband connection.
- Use anti-virus software and check for viruses on their work laptop, memory stick or a CD ROM when transferring information from the internet on a regular basis, especially when not connected to the school/education setting or other establishment's network.

- Ensure that all personal storage devices (i.e. memory sticks) which are utilised by staff members to hold sensitive information are encrypted or password protected in the event of loss or theft.
- Report incidents of personally directed "bullying" or other inappropriate behaviour via the Internet or other technologies using the CMAT accident/incident reporting procedure in the same way as for other non-physical assaults.

5.2 Appropriate and Inappropriate Use by Staff or Adults

- Staff members have access to the network so that they can obtain age appropriate resources for their classes and create folders for saving and managing resources.
- All staff should receive a copy of the Acceptable Use statement and a copy of the Acceptable Use Agreement, which they need to sign, return to the school/education setting or other establishment, to keep under file with a signed copy returned to the member of staff.
- The Acceptable Use Agreement will be displayed in the staff room as a reminder that staff members need to safeguard against potential allegations and a copy of this policy is provided to all staff for home use.

5.3 In the event of inappropriate use, If a member of staff is believed to misuse the internet in an abusive or illegal manner, a report must be made to the Principal/CEO/ Academy Head/Senior Designated Person immediately and then the Managing Allegations Procedure and the Safeguarding Policy must be followed to deal with any misconduct and all appropriate authorities contacted.

6. Children and Young People

6.1 Children should be:

- Responsible for following the Acceptable Use Agreement whilst within school as agreed at the beginning of each academic year or whenever a new child attends the school.
- Taught to use the internet in a safe and responsible manner through Computing, PSHE or other clubs and groups.
- Taught to tell an adult about any inappropriate materials or contact from someone they do not know straight away, without reprimand (age and activity dependent).

6.2 Acceptable Use Agreements and the letter for children, young people and parents/carers are outlined in the Appendices. These detail how children and young people are expected to use the internet and other technologies within school/education setting or other establishment, including downloading or printing of any materials. The agreements are there for children to understand what is expected of their behaviour and attitude when using the internet. This will enable them to take responsibility for their own actions. For example, knowing what is polite to write in an e-mail to another child, or understanding what action to take should there be the rare occurrence of sighting unsuitable material. This also includes the deliberate searching for inappropriate materials and the consequences for doing so.

6.3 School should encourage parents/carers to support the agreement with their child or young person. This can be shown by signing the Acceptable Use Agreements together so that it is clear to the school/education setting or other establishment that the agreement are accepted by the child with the support of the parent/carer. This is also intended to provide support and information to parents/carers when children and young people may be using the Internet beyond school/education setting or other establishment.

6.4 Further to this, it is hoped that parents/carers will add to future rule amendments or updates to ensure that they are appropriate to the technologies being used at that time and reflect any potential issues that parents/carers feel should be addressed, as appropriate.

6.5 The downloading of materials, for example, music files and photographs need to be appropriate and 'fit for purpose' based on research for work and be copyright free.

6.6 In the event of inappropriate use, should a child or young person be found to misuse the online facilities whilst at school, the following consequences should occur:

- Any child found to be misusing the internet by not following the Acceptable Use Agreement may have a letter sent home to parents/carers explaining the reason for suspending the child or young person's use for a particular lesson or activity.
- Further misuse of the agreement may result in not being allowed to access the internet for a period of time and another letter will be sent home to parents/carers.
- A letter may be sent to parents/carers outlining the breach in Safeguarding Policy where a child or young person is deemed to have misused technology against another child or adult.

6.7 In the event that a child or young person **accidentally** accesses inappropriate materials the child should report this to an adult immediately and take appropriate action to hide the screen or close the window, so that an adult can take the appropriate action. Where a child or young person feels unable to disclose abuse, sexual requests or other misuses against them to an adult, they can use the Report Abuse button (www.thinkuknow.co.uk) to make a report and seek further advice. The issue of a child or young person deliberately misusing online technologies should also be addressed by the establishment.

6.8 Children should be taught and encouraged to consider the implications for misusing the internet and posting inappropriate materials to websites, for example, as this may have legal implications.

7 The Curriculum and Tools for Learning

7.1 Internet Use, the school should teach children and young people how to use the Internet safely and responsibly. They should also be taught, through computing and/or PSHE lessons, how to research information, explore concepts and communicate effectively in order to further learning. The following concepts, skills and competencies should have been taught by the time they leave *Year 6:*

(a) Internet literacy.
(b) Making good judgements about websites and e-mails received.
(c) Knowledge of risks such as viruses and opening mail from a stranger.

(d) Access to resources that outline how to be safe and responsible when using any online technologies.
(e) Knowledge of copyright and plagiarism issues.
(f) File sharing and downloading illegal content.
(g) Uploading information – know what is safe to upload and not upload personal information.
(h) Where to go for advice and how to report abuse.

7.2 The National Curriculum is used to teach digital literacy and Online-Safety.

7.3 These skills and competencies are taught within the curriculum so that children and young people have the security to explore how online technologies can be used effectively, but in a safe and responsible manner. Children and young people should know how to deal with any incidents with confidence, as we adopt the 'never blame the child for accidentally accessing inappropriate materials' culture, in the event that they have **accidentally** accessed something.

7.4 Children's personal safety:
Ensuring information uploaded to web sites and e-mailed to other people does not include any personal information such as:

- Full name (first name is acceptable, without a photograph).
- Address.
- Telephone number.
- E-mail address.
- School/education setting or other establishment.
- Clubs attended and where.
- Age or DOB.
- Names of parents.
- Routes to and from school/education setting or other establishment.
- Identifying information, e.g. I am number 8 in the school/education setting or other establishment Football Team.

7.5 Photographs should only be uploaded on the approval of a member of staff or parent/carer and should only contain something that would also be acceptable in 'real life'. Parents/carers should monitor the content of photographs uploaded. Images of children and young people should be stored according to policy.

7.6 Pupils with Additional Learning Needs, the school should strive to provide access to a broad and balanced curriculum for all learners and recognise the importance of tailoring activities to suit the educational needs of each pupil. Where a student has specific learning requirements, or poor social understanding, careful consideration is given to the planning and delivery of Online-Safety awareness sessions and internet access.

8 Trust and School Website

8.1 The uploading of images to the school/education setting or other establishment website should be subject to the same acceptable agreement as uploading to any personal online space. Permission ought to be sought from the parent/carer prior to the uploading of any images. Settings should

consider which information is relevant to share with the general public on a website and use secure areas for information pertaining to specific audiences.

9 E-mail Use

9.1 The school should have E-mail addresses for children to use, as a class and/or as individuals as part of their entitlement to being able to understand different ways of communicating and using computing to share and present information in different forms.

9.2 Individual E-mail accounts can be traced if there is an incident of misuse whereas class e-mail accounts cannot, especially for older users.

9.3 Staff and children should use their school/education setting or other establishment issued e-mail addresses for any communication between home and school. A breach of this may be considered a misuse.

9.4 Parents/carers are encouraged to be involved with the monitoring of E-mails sent, although the best approach with children and young people is to communicate about who they may be talking to and assess risks together.

9.5 Teachers are expected to monitor their class use of E-mails where there are communications between home and school, on a regular (weekly or as necessary) basis. Where an establishment has a network manager, there is an expectation that monitoring software is used to flag up inappropriate terms and that a senior member of the team has an overview of potential issues on a regular basis – refer to the Monitoring section for further information.

10 Mobile Devices

10.1 Staff should be allowed to bring in personal mobile phones or devices for their own use, but **must not use personal numbers to contact children and young people under any circumstances.** Staff must ensure that there is no inappropriate or illegal content stored on the device and should be aware that using features, such as video or sound recording, may be subject to the same procedures as taking images from digital or video cameras.
Staff should be aware that games consoles such as the Sony play station, Microsoft Xbox, Nintendo Wii and DSi and other such systems that have Internet access which may not include filtering, before use within school, authorisation should be sought from the Academy Head and the activity supervised by a member of staff at all times. The school/education setting or other establishment is not responsible for any theft, loss or damage of any personal mobile device.

10.2 School Mobile Devices; The management of the use of these devices should be similar to those stated above, but with the following additions: Where the establishment has provided a mobile device to a member of staff, such as a laptop, PDA or mobile phone, only this equipment should be used to conduct school business outside of the school environment. It should also be policy to ensure that children and young people understand the use of a public domain and the consequences of misuse. Relevant curriculum links should be made to highlight the legal implications and the involvement of law enforcement.

11 Video and Photographs

11.1 Permission must be sought prior to any uploading of images to check for inappropriate content.

11.2 The sharing of photographs via weblogs, forums or any other means online should only occur after permission has been given by a parent/carer or member of staff.

11.3 Any photographs or video clips uploaded should not have a file name of a child, especially where these may be uploaded to a school website. Photographs should only ever include the child's first name although safeguarding guidance states either a child's name or a photograph but not both.

11.4 Group photographs are preferable to individual children and young people and should not be of any compromising positions or in inappropriate clothing. The School will decide how photographs will be used, including where they will be stored (central location which could be viewed by anyone) and when they will be deleted.

11.5 It is current practice by external media such as local and national newspapers to include the full name of children and young people in their publications. Photographs of children should only be used after permission has been given by a parent/carer.

12 Video-Conferencing and Webcams

12.1 Taking images via a webcam should follow the same procedures as taking images with a digital or video camera.

12.2 Permission should be sought from parents and carers if their child is engaged in video conferencing with individuals or groups outside of the school. This process should always supervised by a member of staff and a record of dates, times and participants held by the school/education setting or other establishment.

12.3 Children need to tell an adult immediately of any inappropriate use by another child or adult.

13 Managing Social Networking and Other Web 2.0 Technologies

13.1 Staff and pupils are encouraged to think carefully about the information which they provide on such websites and the way in which it can be manipulated when published (examples of which include Facebook, Twitter and Instagram.)

13.2 In response to this issue the following measures should be put in place:
The school should control access to social networking sites through existing filtering systems.
Students are advised against giving out personal details or information, which could identify them or their location (e.g. mobile phone number, home address, school, groups or clubs attended, IM and E-mail address or full names of friends).

13.3 Students are discouraged from posting personal photos on social networking sites without considering how publicly accessible the information is and the potential for misuse. Advice is also

given regarding background images in photos, which could reveal personal details (e.g. house number, street name, school/education setting or other establishment uniform).
Pupils are advised on social networking security and recommendations made for privacy settings to be activated to 'Friends only' for all applications to restrict unsolicited access. The importance of passwords and blocking of unwanted communications is also highlighted.
The school should be aware that social networking can be a vehicle for cyber bullying. Pupils are encouraged to report any incidents of bullying to the school/education setting or other establishment allowing for the procedures, as set out in the anti-bullying policy, to be followed.

14 Social Networking advice for Staff, Trustees and Governors

14.1 Social networking outside of work hours, on non-school/education setting or other establishment-issue equipment, is the personal choice of all school staff. Owing to the public nature of such websites, it is advisable for staff to consider the possible implications of participation. The following advice should be considered if involved in social networking:

- Personal details are never shared with pupils such as private E-mail address, telephone number or home address. It is recommended that staff ensure that all possible privacy settings are activated to prevent students from making contact on personal profiles. The simplest and most effective way to do this is to remove details from search results and turn off public visibility.
- Staff should not engage in personal online contact with students outside of Trust / school authorised systems (e.g. school E-mail account for homework purposes).
- Staff should ensure that full privacy settings are in place to prevent students from accessing photo albums or personal information.
- Staff are advised against accepting invites from colleagues until they have checked with them in person that the invite is genuine (avoiding fake profiles set up by students).
- There is well documented evidence to suggest that social networking can be a highly effective tool for communicating with students on a **professional** level. Some school/education setting or other establishments, other educational and other settings have set up accounts on Facebook to manage and monitor public and pupil communications through designated members of staff. Other such professional social networking tools include EdModo or Virtual Learning Environments such as Moodle which contain similar features.

15 Safeguarding Measures – Filtering

15.1 Staff, children and young people are required to use the personalised learning space and all tools within it, in an acceptable way. Please refer to the Acceptable Use Agreement for Staff and children and young people for the appropriate use of the school and Trust systems.

15.2 The broadband connectivity has a filter system which should be set at an age appropriate level so that inappropriate content is filtered and tools are appropriate to the age of the child. **All** filtering should be set to 'No Access' within any setting and then controlled via:

- Portal Control (controls filtering at local site level) which controls individual access to the Internet. This also links to the criteria 'Schedule 11' of Level Four site filtering to qualify for access to the broadband services.

- Local Control – controls access to websites and provides the option to add to a 'restrComputinged list'.

15.3 The Academy Head should sign a disclaimer stating agreement to the filtering levels being maintained as part of the connectivity to broadband requirements. In the event that the site level is not set to 'No Access', the Academy Head and Governors should write a letter to the Trust Board to explain how they intend to safeguard their children and young people. E.g. Use an appropriate accredited service such as Netsweeper or school/education setting or other establishment guardian so that the minimum of Beta Level Four is met.

15.4 The levels listed below are in relation to age-appropriate categories:

- Level One E2BN standard basic minimum adult policy.
- Level Two E2BN standard senior pupils' policy.
- Level Three E2BN standard younger pupils' policy.
- Level Four E2BN standard young pupil's policy.
- No search, no politics and religion.

15.5 This complies with the agreed connectivity legalities with Synetrix and E2BN and also ensures our younger audiences are not exposed to unnecessary risks e.g. a blanket Level Two for Primary school/education establishment or other establishment users, is inappropriate.

15.6 Anti-virus and anti-spyware software is used on all network and stand-alone PCs or laptops and is updated on a regular basis.

15.7 A firewall ensures information about children and young people and the school/education or other establishment cannot be accessed by unauthorised users.

15.8 The 'skin' of the online personal space is age appropriate and only tools appropriate to the age of the child are available.

15.9 An RSS (Really Simple Syndication) feed provides a direct link to commonly used websites so that children and young people do not need to leave their personal space for updates.

15.10 Children should use a search engine that is age appropriate such as AskJeeveskids or Yahooligans.

15.11 Links or feeds to e-safety websites are provided.
Hector Protector should be used as a screen cover so that anything accidentally accessed can be covered whilst an adult is informed.

15.12 For older children and young people, the Report Abuse button is available should there be **a concern of inappropriate or malicious contact made by someone unknown. This provides a** safe place for children and young people to report an incident if they feel they cannot talk to a known adult.

15.13 CEOP (Child Exploitation and Online Protection Centre) training for secondary children and young people (and Year 6 Primary children) is annual and part of the PSHE curriculum for raising

awareness on staying safe and being responsible. A link to the www.thinkukknow.co.uk website is part of the skin layout for further advice and information on children or young people's personal online spaces. *Encryption codes on wireless systems prevent hacking.*

16 Tools for Bypassing Filtering

16.1 Web proxies are probably the most popular and successful ways for students to bypass Internet filters today, identifying a cause for concern amongst school/education setting or other establishments, where children and young people can access the Internet. Web proxies also provide an anonymous route through filtering safeguards in existence on networked facilities, allowing users to navigate through potentially harmful or inappropriate content.

16.2 A web proxy is capable of hiding the IP address of the user and opening unrestricted and, in cases, unidentifiable channels through which material can be viewed. The most common use of this tool amongst students is to access social networking features, gaming websites or information of an adult nature- all of which is blocked through the school/education setting or other establishment's filtering system.

16.3 Students and staff are forbidden to use any technology designed to circumvent, avoid or bypass any school/education setting or other establishment security controls (including internet filters, antivirus solutions or firewalls) as stated in the Acceptable Use Agreement.

16.4 Violation of this rule will result in disciplinary or in some circumstances legal action. Please refer to the 'Staff Procedures Following Misuse by Staff/Children and Young People' sections of this document.

16.5 It is worth noting however, that block banning of student's computing or internet access can be severely disruptive to learning across the curriculum and can also affect lesson planning and should only be applied in the most serious breaches.

17 School/Education Setting or Other Establishment Library

17.1 The computers in the school/education setting or other establishment library should be protected in line with the school/education setting or other establishment network.
Where software is used that requires a child login, this ought to be password protected so that the child is only able to access themselves as a user. Children and young people should be taught not to share passwords. The same acceptable use agreement applies for any staff and children and young people using this technology.

18 Parents – Roles

18.1 Each child or young person should receive a copy of the Acceptable Use Agreement on an annual basis or first-time entry to the school which needs to be read with the parent/carer, signed and returned to school, confirming both an understanding and acceptance of the agreement.

18.2 It should be expected that parents/carers will explain and discuss the agreement with their child, where appropriate, so that they are clearly understood and accepted.

18.3 Schools should keep a record of the signed forms.

The Consortium Multi-Academy Trust

Chair of the Members and Board of Trustees: Dawn Carman-Jones
Principal/CEO: Andrew Aalders-Dunthorne
Email: principal@consortiumacademy.org **Tel**: 01379 668283 / 01379 852520

Acceptable Use Agreement for Staff, Governors and Visitors.

This agreement applies to all online use and to anything that may be downloaded or printed. All adults within the school/education setting or other establishment must be aware of their safeguarding responsibilities when using any online technologies, such as the internet, E-mail or social networking sites. They are asked to sign this Acceptable Use Agreement so that they provide an example to children and young people for the safe and responsible use of online technologies. This will educate, inform and protect adults so that they feel safeguarded from any potential allegations or inadvertent misuse themselves.

- I know that I must only use the school/education setting or other establishment equipment in an appropriate manner and for professional uses.
- I understand that I need to give permission to children and young people before they can upload images (video or photographs) to the internet or send them via E-mail.
- I know that images should not be inappropriate or reveal any personal information of children and young people if uploading to the internet.
- I have read the Procedures for Incidents of Misuse so that I can deal with any problems that may arise, effectively.
- I will report accidental misuse.
- I will report any incidents of concern for a child or young person's safety to the Principal/CEO, Academy Head, Senior Designated Person or Online-Safety Lead in accordance with procedures listed in the Acceptable Use Policy.
- I know who my Senior Designated Person is.
- I know that I am putting myself at risk of misinterpretation and allegation should I contact children and young people via personal technologies, including my personal E-mail. I know I should use the school/education setting or other establishment e-mail address and phones (if provided) and only to a child's school/education setting or other establishment e-mail address upon agreed use within the school/education setting or other establishment.
- I know that I must not use the school/education setting or other establishment system for personal use unless this has been agreed by the Principal/CEO, Academy Head and/or Online-Safety Lead.

The Consortium Multi-Academy Trust

Chair of the Members and Board of Trustees: Dawn Carman-Jones
Principal/CEO: Andrew Aalders-Dunthorne
Email: principal@consortiumacademy.org **Tel**: 01379 668283 / 01379 852520

- I know that I should complete virus checks on my laptop and memory stick or other devices so that I do not inadvertently transfer viruses, especially where I have downloaded resources.
- I will ensure that I follow the Data Protection Act 1998 and have checked I know what this involves.
- I will ensure that I keep my password secure and not disclose any security information unless to appropriate personnel. If I feel someone inappropriate requests my password I will check with the Online-Safety Lead prior to sharing this information.
- I will adhere to copyright and intellectual property rights.
- I will only install hardware and software I have been given permission for.
- I accept that the use of any technology designed to avoid or bypass the school/education setting or other establishment filtering system is forbidden. I understand that intentional violation of this rule may result in disciplinary procedures being initiated.
- I have been given a copy of the Acceptable Use Policy to refer to about all Online-Safety issues and procedures that I should follow.

I have read, understood and agree with these Agreement as I know that by following them I have a better understanding of Online-Safety and my responsibilities to safeguard children and young people when using online technologies.

Signed……Date…….

Name (printed)…….

School/education setting or other establishment……

The Consortium Multi-Academy Trust
Chair of the Members and Board of Trustees: Dawn Carman-Jones
Principal/CEO: Andrew Aalders-Dunthorne
Email: principal@consortiumacademy.org **Tel**: 01379 668283 / 01379 852520

My Online-Safety Agreement

This is my agreement for using the internet safely and responsibly.

- I will use the internet to help me learn.
- I will learn how to use the internet safely and responsibly.
- I will only send E-mail messages that are polite and friendly.
- I will only E-mail, chat to or video-conference people I know in the real world or that a trusted adult has approved.
- Adults are aware when I use online tools such as video conferencing.
- I agree never to give out passwords or personal information like my full name, address or phone numbers.
- I agree never to post photographs or video clips without permission or that I will not include my full name with photographs.
- If I need help I know who I can ask and that I can go to www.thinkuknow.co.uk for help if I cannot talk to a trusted adult.
- If I see anything on the internet that makes me feel uncomfortable, I know what to do.
- If I receive a message sent by someone I don't know, I know what to do.
- I know I should follow these guidelines as part of the agreement with my parent/carer.
- I agree to look after myself and others by using my internet in a safe and responsible way.

Signed..... Dated.....

Name.....(Printed)

The Consortium Multi-Academy Trust
Chair of the Members and Board of Trustees: Dawn Carman-Jones
Principal/CEO: Andrew Aalders-Dunthorne
Email: principal@consortiumacademy.org **Tel**: 01379 668283 / 01379 852520

Document Control

Changes History

Version	Date	Amended By	Details of Change

Approval

Name	Job Title	Signed	Date
Andrew Aalders-Dunthorne	Principal/CEO	Electronic signature	24/11/16
Dawn Carman-Jones	On behalf of the Trust Board	Electronic signature	14/15/16

Equality Impact Assessment

Date	Name	Details

END OF DOCUMENT