



SHIRELAND
COLLEGIATE ACADEMY TRUST

Shireland Collegiate Academy Trust Policy Primary Online Safety Policy

| | |
|-----------------------------|--|
| Committee and Date Approved | Trust Board – July 2020 |
| Category | Recommended - DfE |
| Next Review Date | Every two years unless a change in legislation Summer 2022 |
| Policy Availability | Trust Website |
| Officer Responsible | Primary Director for the Trust |

The Trust, all Academies within the Trust and Shireland Learning Limited must comply with this policy.

Contents

| | |
|---|----|
| 1. Scope | 3 |
| 2. Aims..... | 3 |
| 3. Roles and responsibilities | 3 |
| 4. Educating pupils about online safety | 6 |
| 5. Educating parents about online safety | 8 |
| 7. Acceptable use | 8 |
| 8. Mobile devices in academy | 8 |
| 9. Staff using work devices outside academy..... | 8 |
| 10. How the academy will respond to issues of misuse..... | 9 |
| 11. Training..... | 9 |
| 12. Monitoring arrangements | 9 |
| Appendix One: Acceptable Use Agreement for staff, volunteers and visitors. | 10 |
| Appendix Two: Acceptable Use Agreement (pupils and parents/carers) | 13 |

.....

1. Scope

This policy applies to all members of the *academy* community (including staff, pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of academy technologies both in and out of the academy. **Technologies for the purposes of this policy refers to, but is not limited to, devices, systems and the internet.**

This policy is based on the Department for Education's statutory safeguarding guidance, [Keeping Children Safe in Education](#), and its advice for academies on [preventing and tackling bullying](#) and [searching, screening and confiscation](#). It also refers to the Department's guidance on [protecting children from radicalisation](#).

It reflects existing legislation, including but not limited to the [Education Act 1996](#) (as amended), the [Education and Inspections Act 2006](#), the [Equality Act 2010](#) and the [Education Act 2011](#).

The Education and Inspections Act 2006 empowers Headteachers / Principals to such extent as is reasonable, to regulate the behaviour of pupils when they are off the *academy* site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of online-bullying or other Online Safety incidents covered by this policy, which may take place outside of the *academy*, but is linked to membership of the academy. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the [National Curriculum computing programmes of study](#).

2. Aims

Our academy aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and SPC/Trust Board members.
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole academy community in its use of technology.
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

3. Roles and responsibilities

3.1 The Trust Board

The Trust Board has overall responsibility for monitoring this policy and holding the Principal to account for its implementation.

The Trust Board will co-ordinate regular meetings with appropriate staff to discuss online safety and monitor online safety logs as provided by the DSL/Deputy DSL(s).

All members of the Trust Board will:

- Ensure that they have read and understand this policy.
- Agree and adhere to the terms of acceptable use of academy technologies and the internet.

3.2 The Principal and Senior Leaders

The Principal is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the academy.

- The Principal has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety may be delegated to another senior member of school staff or those responsible for safeguarding.
- The Principal and (at least) another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.
- The Principal / Senior Leaders are responsible for ensuring that the relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Principal / Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.

3.3 The Designated Safeguarding Lead

*In some instances, the DSL may be the academy Principal.

Details of the academy's designated safeguarding lead (DSL) and deputy are set out in the Child Protection and Safeguarding Policy.

The DSL/Deputy DSL(s) takes lead responsibility for online safety in the academy, in particular:

- ensuring that staff understand this policy and that it is being implemented consistently throughout the academy
- working with staff, as necessary, to address any online safety issues or incidents
- ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the academy Anti-bullying Policy
- updating and delivering staff training on online safety, liaising with other agencies and/or external services if necessary
- providing regular reports on online safety in the academy to the Principal and/or Standards and Performance Committee

This list is not intended to be exhaustive.

The DSL/Deputy DSL(s) should be trained in Online Safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- online-bullying

3.4 All Staff

Are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current *academy* Online Safety Policy and practices
- they have read, understood, signed and adhere to the Staff Acceptable Use Agreement (AUA)
- they report any suspected misuse or problem to the *Principal or appropriate Senior Leader and/or the DSL/Deputy DSL(s)* for investigation / action / sanction and logging on the appropriate systems.
- all digital communications with pupils / parents / carers should be on a professional level *and only carried out using official school systems*

- online safety issues are embedded in all aspects of the curriculum and other activities
- pupils understand and follow the Online Safety Policy and acceptable use agreements
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc... in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use, processes should be in place for dealing with any unsuitable material that is found in internet searches. Teachers when planning to use the internet as part of lessons will give consideration to a pupils age and stage
- Online safety incidents are logged and dealt with appropriately in line with this policy.
- Incidents of cyber-bullying are dealt with appropriately in line with the academy Anti-bullying Policy

3.5 Technical Support

Technical Support is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at the academy, including terrorist and extremist material
- Ensuring that the academy's technical systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the academy's technical systems on a regular basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

This list is not intended to be exhaustive.

3.6 Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The *academy* will take every opportunity to help parents understand these issues.

Parents are expected to:

- Notify a member of staff or the Principal of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms of acceptable use of academy technologies and the internet.

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues?, UK Safer Internet Centre: <https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues>
- Hot topics, Childnet International: <http://www.childnet.com/parents-and-carers/hot-topics>
- Parent factsheet, Childnet International: <http://www.childnet.com/ufiles/parents-factsheet-09-17.pdf>

3.7 Pupils

* Application of the Online Safety Policy relating to the responsibilities of pupils should always be applied appropriate to the age and stage of the pupils

Pupils:

- are responsible for using academy technologies in accordance with the Student / Pupil Acceptable Use Agreement

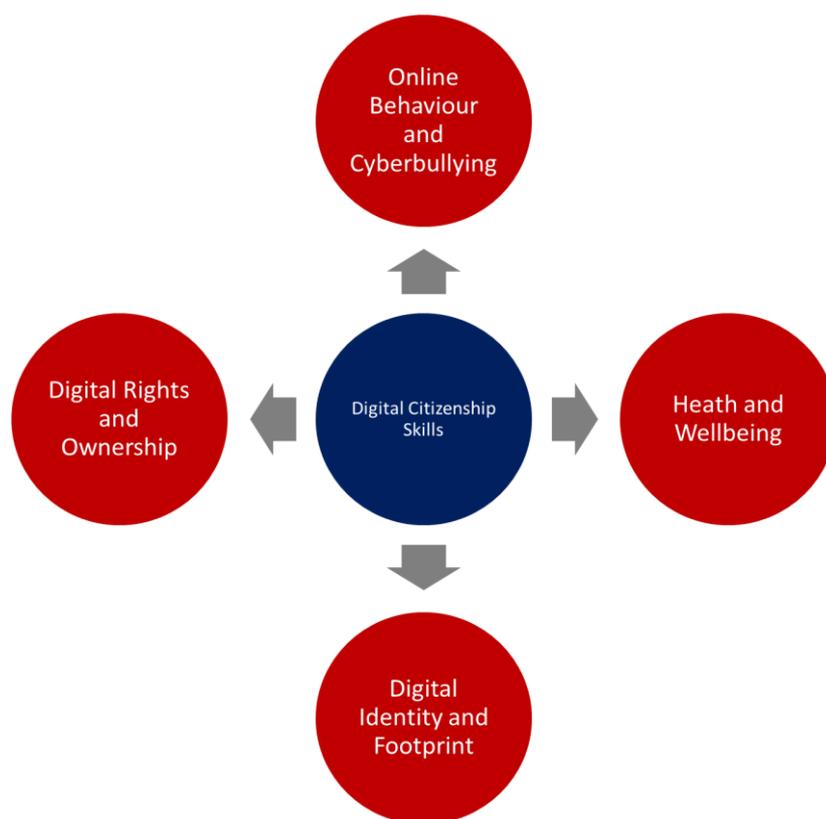
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on online-bullying.
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the *academy's* Online Safety Policy covers their actions out of school, if related to their membership of the school

3.8 Visitors and members of the community

Visitors and members of the community who use academy technologies will be made aware of this policy, when relevant, and are expected to read and follow it. They will be expected to agree to the terms of acceptable use and must sign the Staff /Volunteers Acceptable Use Agreement.

4. Educating pupils about online safety

Pupils will be taught about online safety as part of a wider Digital Citizenship education set out in our Digital Learner Framework:



Pupils will:



| EYFS | KS1 | Lower KS2 | Upper KS2 |
|--|---|--|--|
| <ul style="list-style-type: none"> • Identify emotions of others. <i>e.g. talk about feelings and recognise emotions; consider how actions and words can affect others; realise that behaviour has consequences; identify how they are feeling and know what to do when they feel angry, worried or frightened.</i> • Suggest reasons for likes/dislikes of on- screen activities. • Experience and identify how people can connect with others online. <i>e.g. identify forms of communication (including digital)</i> | <ul style="list-style-type: none"> • Use digital technology to communicate and connect with others. • Identify similarities and differences between online and offline communication. • Begin to interact appropriately with others. <i>e.g. follow the same rules when communicating face-to-face and online.</i> • Start to recognise different symbols seen online. <i>e.g padlock, emoticons.</i> | <ul style="list-style-type: none"> • Take account of the similarities and differences between offline and online communications. <i>e.g. follow the same rules when communicating face-to-face and online; discuss how online communication can be misinterpreted</i> • Identify different forms of bullying, including cyberbullying, and suggest strategies for dealing with it. • Identify actions to report and prevent cyberbullying. • Identify appropriate behaviour when participating in online activities. • Begins to appreciate the need for personal | <ul style="list-style-type: none"> • Demonstrate appropriate online behaviour and apply a range of strategies to protect self and others from possible online dangers, bullying and inappropriate behaviour. <i>e.g. turn off comments on digital media, block users; identify the risks and legal consequences of sending intimate images and content/sexting; recognise language that could be deemed to be offensive (including racist, sexist, homophobic, transphobic) in online activities.</i> |



| EYFS | KS1 | Lower KS2 | Upper KS2 |
|---|---|---|--|
| <ul style="list-style-type: none"> Add their name to digital work Identify work that belongs to others. | <ul style="list-style-type: none"> Add their name and the date to work they have created and give reasons why this is important. <i>e.g. type their first name and surname, add a date to pieces of work and orally provide reasons for doing so.</i> Understand that work produced by other people belongs to them and that it can't be copied without permission. | <ul style="list-style-type: none"> Understand that copying the work of others and presenting it as their own is plagiarism. Explain when and how it is acceptable to use the work of others. <i>e.g. begin to understand the importance of citing the work of others.</i> Understand that work that is produced by some authors can be used if they are acknowledged as the creator. | <ul style="list-style-type: none"> Reference all sources when researching and explain the importance of this. <i>e.g. create simple lists for the referencing of digital and offline sources; discuss rights and permissions associated with this.</i> Understand that there are different categories of digital rights and that these affect usage. <i>E.g. Creative Commons, Copy Right enabled.</i> Understand that content can be edited digitally and discuss rights, permissions and risks associated with sharing digital work online. |



| EYFS | KS1 | Lower KS2 | Upper KS2 |
|---|--|--|---|
| <ul style="list-style-type: none"> Use digital devices and media with care. <i>e.g. name a variety of digital devices and handle appropriately.</i> Recognise that actions have consequences and identify simple rules to keep safe (offline and online). | <ul style="list-style-type: none"> Use digital devices within a controlled environment, time and context. <i>e.g. use for a given time to achieve a specified outcome.</i> Talk about the advantages and disadvantages of digital media in their lives, <i>e.g. on their physical and mental well-being.</i> | <ul style="list-style-type: none"> Acknowledge age restrictions and suitability of digital media and devices. <i>e.g. locate and begin to understand PEGI ratings and age restriction guidelines</i> Identify physical and emotional effects of playing/watching inappropriate content/games. Identify the positive and negative influences of technology on health and the environment. <i>e.g. consider the different ways time is spent and begin to find a balance between active, non-digital and digital activities.</i> Explain the importance of balancing game and screen time with other parts of their lives. Acknowledge that owning a digital device allows you to connect with others both formally and informally. | <ul style="list-style-type: none"> Understand the importance of balancing game and screen time with other parts of their lives. <i>e.g. explore the reasons why they may be tempted to spend more time playing games or find it difficult to stop playing and the effect this has on their health.</i> Reflect on their own media habits and begin to demonstrate healthy online behaviours, identifying unacceptable online behaviour. Understand the importance of balancing being connected to formal and informal networks with personal privacy and well-being. Considers that some people choose to present an edited version (persona and/or images) of themselves online and often these are very different to reality. Appreciates the dangers of using online platforms to chase validation from others. <i>E.g. maximising the number of likes given to a post.</i> |



| EYFS | KS1 | Lower KS2 | Upper KS2 |
|--|---|--|---|
| <ul style="list-style-type: none"> Distinguish between someone they know and someone they have never met. <i>e.g. this links to personal and social education (PSE)/well-being and would form part of 'Stranger Danger' education.</i> Recognise that actions have consequences and identify simple rules to keep them safe (offline and online). <i>e.g. classroom rules/charters should incorporate digital and non-digital rules</i> Begin to understand that information can be shared online. <i>e.g. with adult support, find images of themselves or others online, for example, on the school website/school social media page.</i> | <ul style="list-style-type: none"> Identify private and personal information and discuss how to handle requests for private information Identify the steps that can be taken to keep personal information and hardware secure. <i>e.g. understand usernames and passwords, why we have them and how they are kept safe.</i> Understand that information put Online leaves a digital footprint. | <ul style="list-style-type: none"> Be aware of and apply simple rules for sharing images and data. <i>e.g. understand that photographs cannot be taken of others or shared online without seeking permission first</i> Use effective strategies for creating and keeping strong, secure passwords. Begins to consider how to protect their personal data online. <i>e.g. start to identify risks of sharing and storing passwords, address, phone number etc...</i> Begins to think critically about their digital footprint and the information they leave online | <ul style="list-style-type: none"> Recognise and discuss the impact of sharing digital content, thinking critically about information shared online and develop an awareness of the impact of inappropriate text, photographs and videos. Consider how personal information could be shared unintentionally and the impact this can have on personal reputation, safety and well-being (physical and mental). <i>e.g. metadata and location features and secure websites</i> Thinks critically about their digital footprint and take actions to manage it and appreciates the impact of this on their future. <i>E.g. user accounts, posts, photos etc...</i> |

4.1 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The academy will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss cyber-bullying with their groups, and the issue will be addressed in assemblies.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, SPC/Trust Board members and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

In relation to a specific incident of cyber-bullying, the academy will follow the steps set out in the academy Anti-bullying Policy. Where illegal, inappropriate or harmful material has been spread among pupils, the academy will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

5. Educating parents about online safety

The academy will raise parents' awareness of internet safety in letters or other communications sent home, and in information via our website or Learning Gateway. This policy will also be shared with parents.

Online safety will also be covered during parents' workshops.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the Principal and/or the DSL/ Deputy DSL.

Concerns or queries about this policy can be raised with any member of staff or the Principal.

7. Acceptable use

All pupils, parents, staff, volunteers and SPC members are expected to sign an agreement regarding the acceptable use of academy technologies and the internet. Visitors will be expected to read and agree to the academy's terms of acceptable use if relevant.

Use of the academy's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, SPC members and visitors (where relevant) to ensure they comply with the above.

8. Mobile devices in academy

Pupils are not permitted to bring mobile devices into the academy. Mobile devices brought into academy should be confiscated and returned to the pupils' parent/carer.

Staff are permitted to bring mobile devices into the academy but are not permitted to use their mobile devices around pupils and their families.

9. Staff using work devices outside academy

Staff members using a work device outside of the academy must not install any unauthorised software on the device and must not use the device in any way which would violate the academy's terms of acceptable use.

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside academy. USB devices containing data relating to the academy are not permitted.

If staff have any concerns over the security of their device, they must seek advice from technical support staff.

Work devices must be used solely for work activities.

10. How the academy will respond to issues of misuse

Where a pupil misuses academy technologies or the internet, we will follow the guidance set out in the Behaviour Policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses academy technologies or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The academy will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

11. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

The DSL and Deputy DSL will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Trust Board members will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our Child Protection and Safeguarding Policy.

12. Monitoring arrangements

The DSL/Deputy DSL logs behaviour and safeguarding issues related to online safety.

This policy will be reviewed bi-annually by Shireland Collegiate Academy Trust alongside academy Principals and/or the DSL/ Deputy DSL. At every review, the policy will be shared with the Standards and Performance Committee and Trust board.

Appendix One: Acceptable Use Agreement for staff, volunteers and visitors.

Acceptable use of the academy technologies including devices, systems and the internet: agreement for staff, volunteers and visitors

Name:

Staff / Volunteer / Visitor Acceptable Use Agreement

Introduction

New technologies have become integral to the lives of children and young people in today's society, both within the Academy and in their lives outside the Academy. 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. They also bring opportunities for staff to be more creative and productive in their work. All users have an entitlement to safe internet access at all times.

This Acceptable Use Agreement is intended to ensure that:

- Staff, volunteers and visitors will be responsible users and stay safe while using the internet and other communication technologies for educational, personal and recreational use.
- Academy technologies (including, but not limited to, devices and systems) and users are protected from accidental and / or deliberate misuse that could put the security of the systems or safety of users at risk.
- Staff are protected from potential risk in their use of technology in their everyday work.

The Academy will try to ensure that staff and volunteers will have good access to technology to enhance their work, to enhance learning opportunities for pupils and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Agreement

I understand that I must use technology in a responsible way, to ensure that there is no risk to my safety or to the safety and security of other users and / or academy technologies. I recognise the value

of the use of technology for enhancing teaching and learning, creating efficiencies and reducing workload, and will ensure that pupils receive opportunities to gain from the use of technology. I will, wherever possible, educate the young people in my care in the safe use of technology and embed online safety in all aspects of my work with young people. I will have an up to date awareness of online safety matters and of the current academy Online Safety Policy and practices.

For my professional and personal safety:

- I understand that the academy will monitor my use of technology, including, but not limited to, the monitoring of digital communications including email, the use of academy devices and the use of the internet on academy devices and systems (i.e. academy internet connections etc) using software such as Smoothwall.
- I understand that the rules set out in this agreement apply to the use of all academy technologies including, but not limited to, devices and systems i.e. laptops, iPads, O365, MIS etc...) both inside and outside of the academy.
- I understand that all technology within the academy are intended for educational use or the operations of the academy.
- I will not disclose any of my usernames or passwords to anyone else, nor will I try to use any other person's username and password.
- I will immediately report any illegal, inappropriate or harmful material or incident I become aware of.
- I will report any suspected misuse for investigation / action / sanction and ensure that incidents are logged in accordance with the appropriate academy policies.

I will be professional in my communications and actions when using academy systems:

- I will not access, copy, remove or otherwise alter any other user's files, without permission, unless shared for the purpose of collaboration or in the spirit of reducing workload.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with all relevant Trust, Phase or Local policies I will not use my personal equipment to record images, unless I have permission to do so. Where these images are published, it will not be possible to identify by name, or other personal information, those who are featured.
- I will not use social media sites/apps within the academy unless prior approval has been granted and use is in line with my role.
- I will only communicate with pupils / parents / carers using official academy systems. Any such communication will be professional in tone and manner.
- I will not share any personal information with a pupil.
- I will not communicate with any current pupils digitally other than through sites set up by the Shirland Collegiate Academy Trust via O365. Any such communications will be professional in nature and in line with my role.
- I will not request, or respond to, any personal information from a pupil, other than that which might be appropriate as part of the professional role.
- I will ensure that all communications are transparent and open to scrutiny.
- I will not give out my personal contact details to pupils, including, but not limited to, my mobile telephone number, personal email addresses, social media profiles and details of any blogs/vlogs or personal websites/channels.
- I will not accept or invite pupils as 'friends' on social media sites or apps and must delete any of these young people currently accepted as 'friends' on any social media sites or apps.
- I will review 'friend lists' regularly and remove any current pupils or person under the age of 18 years where it could be perceived as inappropriate to maintain contact with that young person.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The academy has the responsibility to provide safe and secure access to technologies and to ensure the smooth running of the academy:

- I will not connect personal devices to academy systems.
- I will not use storage devices to store and/or transport sensitive documents including those containing pupil data or information.
- I will avoid the use of USB sticks where possible opting to use OneDrive or O365 in order to access files.
- I will not open any attachments to online communications such as emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- I will ensure that my data and files on academy devices are regularly backed up, in accordance with relevant academy policies. I will endeavour to use OneDrive to store files avoiding the need for files or data to be stored on the device.
- I will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others (child sexual abuse images, criminally racist material, adult pornography). I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes or software of any type on a machine, or store programmes or software on a computer, nor will I try to alter computer settings.
- I will not disable or cause any damage to academy equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the Trust Data Protection Policy. Any transferring of data outside of the academy will be in line with the Trust Data Protection Policy.
- I understand that the Trust Data Protection Policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by the Trust Data Protection Policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened, regardless of fault.

When using the internet in my professional capacity or for academy sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music, images and videos).

I understand that I am responsible for my actions in and out of the academy:

- I understand that this Acceptable Use Agreement applies not only to my work and use of academy technologies in the academy, but also applies to my use of academy technologies outside of the academy and my use of personal equipment in the academy or in situations related to my employment by the academy.
- I understand that if I fail to comply with this Acceptable Use Agreement, I could be subject to disciplinary action.

I have read and understand the above and agree to use academy technologies (both inside and outside of the academy) and my own devices (in the academy and when carrying out communications related to the academy) within these guidelines.

Staff / Volunteer Name:

Signed:

Date:

*Academy technologies refers to all hardware, software and technical systems including internet access. Examples include, but are not limited to laptops, iPads, mobile phones, MIS and O365

Appendix Two: Acceptable Use Agreement (pupils and parents/carers)

Acceptable use of the academy technologies including devices, systems and the internet: agreement for pupils and parents/carers

Name of pupil:

For pupils in Key Stage Two and all parent/carers:

When using academy technologies, including devices such as laptops or tablets, systems such as the Learning Gateway and accessing the internet in the academy, I will not:

- Use them for a non-educational purpose.
- Use them without a teacher being present, or without a teacher's permission.
- Access any inappropriate websites and/or apps. When accessing the internet, I will consider the 'Think Before You Click' approach.
- Access recreational or social/communication websites or apps (unless directed to as part of a learning activity).
- Open any attachments in online communications such as emails, or follow any links, without first checking with a teacher.
- Use any inappropriate language when communicating online.
- Share my password with others or log into the academy systems (such as the Learning Gateway) using someone else's details.
- Give my personal information (including my name, address or telephone number) to anyone without the permission of my teacher or parent/carer.
- Arrange to meet anyone I have met online in person without first consulting my parent/carer, and without adult supervision. I will be aware of 'stranger danger' when communicating online.
- I will not bring a personal mobile phone or other personal device into the academy.

I agree that the academy will monitor the websites and apps that I visit.

I will immediately let a teacher or other member of staff know if I find any material which might upset, distress or harm me or others.

I will always use academy technologies and the internet responsibly.

For pupils in EYFS and Key Stage One:

- I will ask a teacher or suitable adult if I want to use any technology such as computers or tablets.
- I will only use activities that a teacher or suitable adult has asked or allowed me to use.
- I will take care of all equipment.
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong.
- I will tell a teacher or suitable adult if I see something that upsets me on the screen.
- I know that if I do not meet the expectations I might not be allowed to use technology.

Signed (pupil):

Date:

Parent/carer agreement: I agree that my child can use academy technologies and the internet when appropriately supervised by a member of academy staff. I agree to the conditions set out above for pupils using academy technologies and the internet and will make sure my child understands these.

Signed (parent/carer):

Date: