Shireland Collegiate Academy Trust Policy

Primary Online Safety Policy

Committee and Date Approved	Trust Board – Summer 2024
Category	Recommended - DfE
Next Review Date	Every two years unless a change in legislation **Summer 2026**
Policy Availability	Trust Website
Officer Responsible	Primary Director for the Trust

Contents

1. Scope

This policy applies to all stakeholders of the Shireland Collegiate Academy Trust's primary academies (including staff, pupils, volunteers, parents/carers, visitors and community users) who have access to and are users of academy integrated technologies both in and out of academy sites.

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 Teaching online safety in schools; Preventing and tackling bullying 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 and cyber-bullying: advice for headteachers and school staff.

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

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and SPC/Trust Board.

- Identify and support groups of pupils that are potentially at greater risk of harm online than others.

- 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.

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism.
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
- **Conduct** – personal online behaviour that increases the likelihood of, or causes harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying.
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

3. Roles and responsibilities

3.1 The Standards and Performance Committee

The Standards and Performance Committee has the overall responsibility for monitoring this policy and holding the Principal to account for its implementation and will report to the Trust Board.

The Standards and Performance Committee 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 Standards and Performance Committee will:

- Monitor the implementation of this policy.
- Agree and adhere to the terms of acceptable use of academy technologies and the internet.
- Ensure that online safety is a running and interrelated theme while devising and implementing the approach to safeguarding and related policies.
- Check that all academy staff complete online safety training as part of child protection and safeguarding training and ensure staff understand their expectations, roles and responsibilities regarding filtering and monitoring online activities through (SENSO) software.
- Review training records to ensure staff are provided with regular online safety updates through channels such as email, e-bulletins, portal training and staff meetings, to enhance their capability to effectively protect and safeguard children in the digital age.
- Visit academies and view pupil voice to see how children are educated to keep themselves and others safe, including online safety.

- Ensure the academy uses their SENSO filtering and monitoring systems on their devices and networks, regularly assessing their efficiency and reviewing the Department for Education's filtering and monitoring standards, engaging with IT personnel and service providers to meet the requirements, which encompass:
  - Allocating roles and duties for managing filtering and monitoring systems.
  - Conducting annual reviews of filtering and monitoring provisions.
  - Blocking harmful content while minimising disruption to teaching and learning.
  - Implementing monitoring strategies that cater to safeguarding requirements.

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 and on each academy’s website.

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 or inappropriate online behaviours are logged and dealt with appropriately in line with the Primary Anti-bullying or Behaviour 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:
    - liaising with external agencies when needed.
    - conducting annual risk assessments focusing on children's risks.

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 and Volunteers

All staff, including contractors, agency staff and volunteers are responsible for:

- Maintaining an understanding of this policy.

- Implementing this policy consistently.

- Accessing up-to-date awareness of online safety matters and of the current Online Safety Policy and practices.

- Signing and adhering to the Staff Acceptable Use Agreement (AUA).

- Reporting 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 being embedded in all aspects of the curriculum and other activities they deliver.

- Ensuring that pupils understand and follow the Online Safety Policy and acceptable use agreements.

- Supporting pupils to have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.

- Monitoring the use of digital technologies (such as mobile devices, cameras, etc) in lessons and other school activities (where allowed) and implement current policies with regard to these devices.

- Adequate supervision in lessons where internet use is pre-planned, ensuring pupils are 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 consider a pupil’s age and stage.

- Logging online safety incidents including cyber-bullying and ensuring that they are dealt with appropriately in line with our academy policies and procedures.

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.

- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy.

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
- Hot topics - Childnet
- Parent resource sheet - Childnet
- General parental information: Parents and carers | CEOP Education (thinkuknow.co.uk)

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:

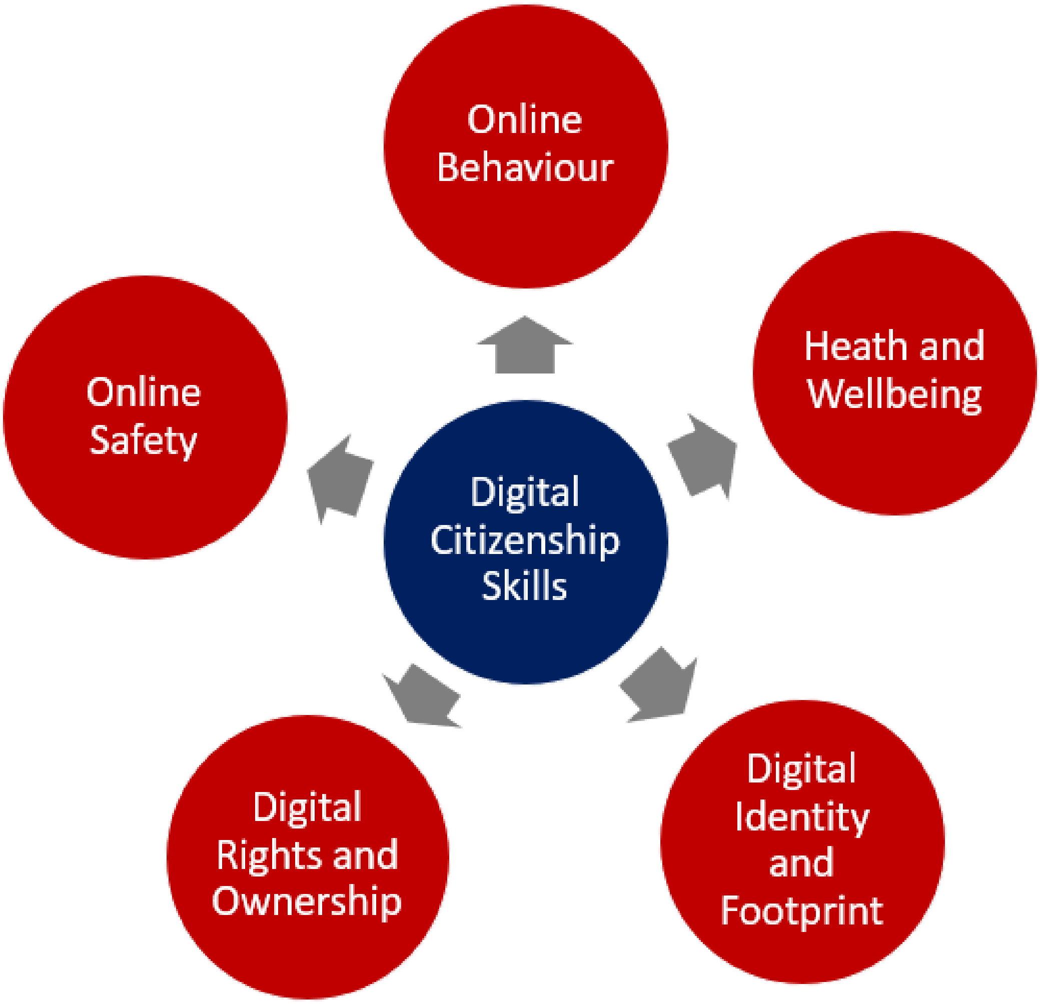
- Are responsible for using academy technologies in accordance with the Student / Pupil Acceptable Use Agreement.
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- Need to understand the importance of reporting abuse, misuse or access 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 Primary 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:


Online Behaviour
Heath and Wellbeing
Online Safety
Digital Citizenship Skills
Digital Rights and Ownership
Digital Identity and Footprint

Pupils will:

Digital Citizenship Skills

*Online Behaviour and Cyberbullying

EYFS	KS1	Lower KS2	Upper KS2
- Identify emotions of others. 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 felling and know what to do when they feel angry, worried or frightened. - Suggest reasons for likes/dislikes of on- screen activities. - Experience and identify how people can connect with others online. e.g. identify forms of communication (including digital)	- Use digital technology to communicate and connect with others. - Identify similarities and differences between online and offline communication. - Begin to interact appropriately with others. e.g. follow the same rules when communicating face-to-face and online. - Start to recognise different symbols seen online. e.g padlock, emoticons.	- Take account of the similarities and differences between offline and online communications. e.g. follow the same rules when communicating face-to-face and online; discuss how online communication can be misinterpreted. - Identify different forms of bullying, including cyberbullying, and suggest strategies for dealing with it. - Identify actions to report and prevent Cyberbullying / inappropriate online behaviour - Identify appropriate behaviour when participating in online activities. - Begins to appreciate the need for personal responsibility and safety when online. E.g. considers sign up age/requirements before joining social media and downloading apps etc. - Appreciate that inappropriate online behaviour has consequences offline.	- Demonstrate appropriate online behaviour and apply a range of strategies to protect self and others from possible online dangers, bullying and inappropriate behaviour. 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.

Digital Citizenship Skills

Digital Rights and Ownership

EYFS	KS1	Lower KS2	Upper KS2
• Add their name to digital work. • identify work that belongs to others.	• Add their name and the date to work they have created and give reasons why this is important. *e.g. type their first name and surname, add a date to pieces of work and orally provide reasons for doing so.* • Understand that work produced by other people belongs to them and that it can't be copied without permission.	• 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. *e.g begin to understand the importance of citing the work of others.* • Understand that work that is produced by some authors can be used if they are acknowledged as the creator.	• Reference all sources when researching and explain the importance of this. *e.g. create simple lists for the referencing of digital and offline sources; discuss rights and permissions associated with this.* • Understand that there are different categories of digital rights and that these affect usage. *E.g. Creative Commons, Copy Right enabled.* • Understand that content can be edited digitally and discuss rights, permissions and risks associated with sharing digital work online.

Digital Citizenship Skills

*Health and Wellbeing

EYFS	KS1	Lower KS2	Upper KS2
- Use digital devices and media with care. e.g. name a variety of digital devices and handle appropriately. - Recognise that actions have consequences and identify simple rules to keep safe (offline and online).	- Use digital devices within a controlled environment, time and context. e. g use for a given time to achieve a specified outcome Yr 1/2. - Talk about the advantages and disadvantages of digital media in their lives, e.g. on their physical and mental well-being.	- Acknowledge age restrictions and suitability of digital media and devices. e.g. locate and begin to understand PEGI ratings and age restriction guidelines. - Identify physical and emotional effects of playing/watching inappropriate content/games. - Identify the positive and negative influences of technology on health and the environment. e.g. consider the different ways time is spent and begin to find a balance between active, non-digital and digital activities. - Explain the importance of balancing game and screen time with other parts of their lives. - Begin to consider the ways in which companies try to keep you online for longer periods of time e.g. persuasive design, in-app purchases, clickbait. - Acknowledge that owning a digital device allows you to connect with others both formally and informally.	- Understand the importance of balancing game and screen time with other parts of their lives. 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. - 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. E.g. maximising the number of likes given to a post.

Digital Citizenship Skills

*Digital Identity and Footprint

EYFS	KS1	Lower KS2	Upper KS2
• Distinguish between someone they know and someone they have never met. e.g. this links to personal and social education (PSE)/well-being and would form part of 'Stranger Danger' education. • Recognise that actions have consequences and identify simple rules to keep them safe (offline and online). e.g. classroom rules/charters should incorporate digital and non-digital rules. • Begin to understand that information can be shared online. e.g. with adult support, find images of themselves or others online, for example, on the school website/school social media page.	• Identify private and personal information and discuss how to handle requests for private information. Yr 1/2. • Identify the steps that can be taken to keep personal information and hardware secure. e.g. understand usernames and passwords, why we have them and how they are kept safe. Yr 1/2. • Understand that information put online leaves a digital footprint. • Begin to consider benefits and risks of sharing online	• Be aware of and apply simple rules for sharing online including images, videos, text and data. e.g. understand that photographs cannot be taken of others or shared online without seeking permission first. • Use effective strategies for creating and keeping strong, secure passwords. Yr 1/2. • Begins to consider how to protect themselves online. e.g. start to identify risks of sharing and storing passwords, and other personal information.Yr 1/2 • Consider their safety when posting digital content i.e., images/videos. • Begins to think critically about their digital footprint and the information they leave online.	• 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). e.g metadata and location features and secure websites. • Thinks critically about their digital footprint and take actions to manage it and appreciates the impact of this on their future. E.g user accounts, posts, photos etc…

Information taken from Education for a Connected World 2020 edition (As referenced by Teaching online safety in schools DfE website)

EYFS	KS1	Lower KS2	Upper KS2
Self-image and identity • Recognise the differences between online or offline, that anyone can say 'no' / 'please stop' / 'I'll tell' / 'I'll ask' to somebody who makes them feel sad, uncomfortable, embarrassed or upset. Digital Citizenship Skills Online Safety	**Self-image and identity** • Give examples of who to talk too when experiencing feelings of sadness, worry, or frightened. • Explain how other people may look and act differently online and offline • Give examples of issues online that might make someone feel sad, worried, uncomfortable or frightened; give examples of how they might get help.	**Self-image and identity** • Explain what is meant by the term 'identity'. • Explain how people can represent themselves in different ways online. • Explain ways in which someone might change their identity depending on what they are doing online (e.g. gaming; using an avatar; social media) and why. • Explain how online identity can be different to offline identity. • Describe positive ways for someone to interact with others online and understand how this will positively impact on how others perceive them. • Explain that others online can pretend to be someone else, including friends, and can suggest reasons why they might do this.	**Self Image and identity** • Explain how identity online can be copied, modified or altered. • Demonstrate how to make responsible choices about having an online identity, depending on context. • Identify and critically evaluate online content relating to gender, race, religion, disability, culture and other groups, and explain why it is important to challenge and reject inappropriate representations online. • Describe issues online that could make anyone feel sad, worried, uncomfortable or frightened. Know and can give examples of how to get help, both on and offline. • Explain the importance of asking until the required help needed.

Information taken from Education for a Connected World 2020 edition (As referenced by **Teaching online safety in schools DfE website**)

EYFS	KS1	Lower KS2	Upper KS2
Online relationships • Recognise some ways in which the internet can be used to communicate. • Give examples of how technology can be used to communicate with people • Give examples of when permission should be granted to put something online and explain why this is important. • Use the internet with adult support to communicate with people who are known (e.g. video call apps or services). • Explain why it is important to be considerate and kind to people online and to respect their choices. • Explain why things one person finds funny or sad online may not always be seen in the same way by others. 	**Online relationships** • Give examples of how someone might use technology to communicate with others they don't also know offline and explain why this might be risky. (e.g. email, online gaming, a pen-pal in another school / country). • Explain who can give consent before sharing things about myself or others online. • Describe different ways to ask for, give, or deny permission online and can identify who can help when unsure • Explain that people have a right to say 'no' or 'I will have to ask someone'. Explain who can help when experiencing feelings of being under pressure to agree to something when unsure about or don't want to do. • Identify who can help if something happens online without consent. • explain how it may make others feel their permission is not asked for or their answers are ignored before sharing something about them online. • explain why a trusted adult should be asked before clicking 'yes', 'agree' or 'accept' online.	**Online relationships** • Describe ways people who have similar likes and interests can get together online. • Explain what it means to 'know someone' online and why this might be different from knowing someone offline. • Explain what is meant by 'trusting someone online', why this is different from 'liking someone online', and why it is important to be careful about who to trust online including what information and content they are trusted with. • Explain why someone may change their mind about trusting anyone with something if they feel nervous, uncomfortable or worried. • Explain how someone's feelings can be hurt by what is said or written online. • Explain the importance of giving and gaining permission before sharing things online; how the principles of sharing online is the same as sharing offline e.g. sharing images and videos • Describe strategies for safe and fun experiences in a range of online social environments e.g. livestreaming, gaming platforms • Give examples of how to be respectful to others online and describe how to recognise healthy and unhealthy online behaviours. • Explain how content shared online may feel unimportant to one person but may be important to other people's thoughts feelings and beliefs.	**Online relationships** • Give examples of technology- specific forms of communication (e.g. emojis, memes and GIFs). • Explain that there are some people online may want to do harm. Recognise that this is not my / our fault. • Describe some of the ways people may be involved in online communities and describe how they might collaborate constructively with others and make positive contributions. (e.g. gaming communities or social media groups). • Explain how someone can get help if they are having problems and identify when to tell a trusted adult. • Demonstrate how to support others (including those who are having difficulties) online. • Explain how sharing something online may have an impact either positively or negatively. • Describe how to be kind and show respect for others online including the importance of respecting boundaries regarding what is shared about them online and how to support them if others do not. • Describe how things shared privately online can have unintended consequences for others. e.g. screen-grabs. • Explain that taking or sharing inappropriate images of someone (e.g. embarrassing images), even if they say it is okay, may have an impact for the sharer and others; and who can help if someone is worried about this.

Information taken from Education for a Connected World 2020 edition (As referenced by **Teaching online safety in schools DfE website)**

EYFS	KS1	Lower KS2	Upper KS2
Online reputation • Identify ways that information on the internet 	**Online reputation** • Recognise that information can stay online and could be copied. • Describe what information should not put online without asking a trusted adult first. • Explain how information put online about someone can last for a long time. • Describe how anyone's online information could be seen by others. • Know who to talk to if something has been put online without consent or if it is incorrect.	**Online reputation** • Explain how to search for information about others online. • Give examples of what anyone may or may not be willing to share about themselves online. I can explain the need to be careful before sharing anything personal. • Explain who someone can ask if they are unsure about putting something online.	**Online reputation** • Search for information about an individual online and summarise the information found. • Describe ways that information about anyone online can be used by others to make judgments about an individual and why these may be incorrect. • Explain the ways in which anyone can develop a positive online reputation. • Explain strategies anyone can use to protect their 'digital personality' and online reputation, including degrees of anonymity.

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, Trustees, Governors, 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 Primary 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.

Educating parents/families about online safety

Primary academies within the Trust will share this policy with parents/families to raise awareness of internet safety.

The following information will be communicated to parents/families:

- What systems are being used in the academy to filter and monitor online use.
- What children are being asked to do online (e.g., sites they need to visit or who they will be interacting with online).

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.

4.2 Examining electronic devices

The authority to search and confiscate electronic devices within the school premises lies with the Principal or any senior staff member authorised by the Principal, as outlined in the behaviour policy. When there are reasonable grounds to suspect that an electronic device:

- Poses a risk to staff or pupils.
- Violates school rules by being a banned item subject to search.
- Is linked to potential evidence of an offence.

Before conducting a search, authorised staff must assess the urgency of the situation and potential risks to others. If the search is non-urgent, consultation with appropriate personnel is required. The pupil must be informed of the reasons for the search, its procedure and given the chance to ask questions, while their cooperation is sought.

In exceptional cases, authorised staff may examine or erase data from confiscated devices if there is a 'good reason'. This includes suspecting the device could:

- Cause harm.
- Disrupt the school's safe environment.
- Be involved in criminal activities.

Should inappropriate material be found, a suitable response will be determined by the staff member in conjunction with the DSL, Principal or senior leadership team. If the material poses a risk, safeguarding measures will be prioritised. When considering erasing data, leaders will assess if it could serve as evidence for an offence. If not, and the data's existence could lead to harm, deletion can take place if the pupil or parent/carer declines to do so. However, potential evidence related to an offence must be preserved and handed over to the police promptly.

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image.
- Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people.

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation.
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people.
- Our behaviour policy

4.3 Artificial Intelligence (AI)

Artificial intelligence (AI) tools such as ChatGPT and Google Bard have become increasingly prevalent and easily accessible to staff, pupils, and parents/carers. While AI presents various benefits for enhancing learning experiences, it also brings forth potential risks concerning online safety, particularly in the domain of bullying.

Shireland Collegiate Academy Trust acknowledges the multifaceted nature of AI and its implications for pupil welfare. One significant concern is the misuse of AI in perpetrating acts of bullying through techniques like 'deepfakes'. Deepfakes utilise AI algorithms to craft deceptive images, audio, or videos that closely resemble reality. In some cases, this information can be used to produce explicit content featuring individuals' likenesses without their consent.

In line with our existing anti-bullying/behaviour policies, Shireland Collegiate Academy Trust is committed to addressing any instances of AI-enabled bullying promptly and decisively. The safeguarding of pupils in the digital realm is paramount, and any misuse of AI to harm or intimidate others will not be tolerated within our school communities.

To uphold a safe online environment, staff will be made aware of the potential risks associated with AI tools, especially as new technologies continue to evolve. Conducting thorough risk assessments when integrating any type of AI applications into school practices to mitigate potential harm and maintain a secure digital space for all pupils.

5. 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 governors and visitors (where relevant) to ensure they comply with the above.

6. 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.

7. 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.

8. 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 Primary 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.

9. 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.

Trustees 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 each academy's Child Protection and Safeguarding Policy.

11. Monitoring arrangements

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

This policy will be reviewed by Shireland Collegiate Academy Trust alongside academy Principals and/or the DSL/Deputy DSL as per the frequency stated on the front cover. At every review, the policy will be shared and approved by the 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 is 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:**