CASTLEWARD
SPENCER ACADEMY

CASTLEWARD
SPENCER ACADEMY

E-Safety Policy

September 2021.

This policy will be reviewed annually- it is linked to the following polices; Safeguarding, Behaviour, Anti-bullying, PSHE and Computing.

SPENCER
ACADEMIES TRUST

Introduction

This policy applies to all members of the school community (including staff, pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of our ICT systems, both in and out of the school. The Education and Inspections Act 2006 empowers principals to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other E-Safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data.

Castleward Spencer Academy will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate E-Safety behaviour that take place out of school.

Roles and Responsibilities

The following section outlines the E-Safety roles and responsibilities of individuals and groups within the school.

Principal

The Principal is responsible for monitoring the teaching of computing and online safety throughout the school. They will also oversee the completion of the computing concepts in each year group.

Computing Lead

The computing lead will oversee planning in all year groups throughout the school and be responsible for raising standards in computing and online safety. They will also be responsible for informing staff of new developments and initiatives and providing training where appropriate. The computing lead is responsible for overseeing the assessment of computing across the school and providing opportunities to moderate computing ability.

Teachers

Other subject leaders and classroom teachers should be aware that it is their responsibility to plan and teach computing and online safety and to use computing within their class. This will be in accordance to the schemes of work provided by the computing lead. They will also assist in the monitoring and recording of pupil progress in computing. Teachers should also respond to, and report, and E-Safety or cyber bullying issues that they encounter within or out of school in accordance to E-Safety procedures as listed below. Staff should follow, and agree to the Acceptable Usage Policy, see appendix.

Governors and visitors

School governors should abide by the guidelines set out for staff and ensure that if they do use the computers and equipment within school that they are doing so safely.

The School

As a school, we will endeavour to ensure that parents and pupils are fully aware of ways in which the internet and computing can be used productively and safely. We will always ensure that we provide children with the opportunities to excel and achieve when using computing and will ensure our curriculum is challenging and relevant. Before launching any system or initiative, we will make sure that the children's safety is at the forefront of our thoughts and we will keep parents informed as necessary through letters, Class Dojo, texts and parents' events.

Pupils

Pupils should follow the school internet use guidelines. They should ensure that they use the computers and equipment appropriately at all times. It is expected that children will follow the school's behaviour policy when working online. They are also expected to adhere to the school's Anti-bullying policy. If the children fail to do so, then the procedures outlined in these policies will come into force.

Parents

Parents should stay vigilant to the websites and content that their children are accessing. They should also try to talk to their child about E-Safety and the use of the internet. If they have any questions or concerns then they should speak to their child's teacher, the computing lead or the Principal.

Internet

The internet may be accessed by staff and by children throughout their hours in school. We ask as a school that staff are vigilant as to the sites children are accessing and children should not be using the internet unattended.

The teaching of email and internet use will be covered within the computing curriculum planning, but staff should encourage regular dialogue that explores the benefits and potential dangers of using the internet.

All members of staff will be issued with a school email address and this is the email with which they should use for professional communication. Staff should take extra care to ensure that all communication with children and/or parents remains professional. Users are responsible for all messages that are sent and due regard should be paid to the content of the emails to ensure it is not misconstrued. All web activity is monitored by the computing lead, so it is the user's responsibility to ensure they log off appropriately.

The use of the internet to access inappropriate materials such as auction sites, pornography, racist or any other material is prohibited. If users, especially children, do see an inappropriate website or image, they should close this immediately and report the site to their class teacher who will subsequently report it to the ICT support team.

Inappropriate websites are filtered out by AIT (Advanced IT Services)

Online Safety lessons

Today's pupils are growing up in an increasingly complex world, living their lives seamlessly on and offline. This presents many positive and exciting opportunities, but also challenges and risks. It is important to teach pupils about the underpinning knowledge and behaviours that can help pupils to navigate the online world safely and confidently regardless of the device, platform or app.

It is crucial that we regularly promote "Be SMART" and this should be a reminder at the beginning of every computing session. At CWSA we have a Long Term Plan to teach Online Safety. This is taught every other week and the planning from Project Evolve will be used an adapted for our pupils. It is vital we teach each element of the Online Safety plan to ensure children have a firm grasp of Online Safety keeping emerging needs in mind. Our long term plan takes a flexible approach to meet the needs of the children. Every half term we have an assembly, which is based on the strand we are focusing on for that term. *THE STRANDS CAN BE MOVED TO MEET THE NEEDS OF YOUR CHILDREN.

Passwords

Staff should make sure that any passwords they use are strong and contain a mixture of some of the following; upper- and lower-case letters, numbers and punctuation. These should be changed regularly, especially if the user suspects others may know the password.

For sites where children have passwords, e.g. Purple Mash, they will be provided with these by the computing lead. As children progress through the school they will be taught about having sensible passwords.

Email

Electronic mail (email) is an essential communication mechanism for both staff and pupils in today's digitally-connected world. The use of email can bring significant educational benefits for any school, both for its staff and pupils. However, email use for staff and pupils needs to be thought through and appropriate safety measures put in place.

Staff and pupils should only use approved email accounts allocated to them by the school and should be aware that any use of the school email system will be monitored and checked. Staff should not use personal email accounts during school hours or for professional purposes, especially to exchange any school-related information or documents. (unless granted permission from the Principal).

It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged. A full audit trail can be made available should this become necessary. Under no circumstances should staff contact pupils, parents or conduct any school business using personal email addresses.

When learning about emails, pupils will use Purple Mash 2 email.

- Pupils and staff will be reminded when using email about the need to send polite and responsible messages.
- Pupils and staff will be reminded about the dangers of revealing personal information within email conversations.
- Emails containing personal, confidential, classified or financially sensitive data to external third parties or agencies needs to be controlled and never communicated through the use of a personal account.
- All confidential documents sent between staff via email will be password protected.
- Pupils and staff will be made aware of the dangers of opening email from an unknown sender or source or viewing and opening attachments.
- All emails should be written and checked carefully before sending, in the same way as a letter written on school-headed paper.
- Staff who send emails to external organisations or parents, are advised to carbon copy (cc) or include the Principal, line manager or another suitable member of staff into the email.

Social Media

As a school, we fully recognise that social media and networking are playing an increasing role within every-day life and that many staff are users of tools such as Facebook, Twitter and blogs using these for both personal and professional use. We will ensure that staff and children are kept fully aware of risks and issues that may arise and ways in which to minimise these risks.

Staff should:

- Ensure that their profile/posts are kept private to friends where possible, this also includes personal information such as phone numbers, email addresses etc.

- Not accept current or ex-pupils or parents as ‘friends’ on social media sites such as Facebook. This is to ensure any possible misinterpretation. We do understand that some staff members

have friends within the local community (such as children's parents) and ask that these members of staff take extra precaution when posting online.

- Ensure that if their communication is fully public (e.g. blogs/Twitter), that they maintain their professionalism at all times and remember that they are a representative of the school
- Be aware that electronic texts can sometimes be misinterpreted or misconstrued so should endeavour to minimise the possibility of this happening
- Not use these media to discuss confidential information or to discuss specific children
- Check with the computing lead if they need advice on monitoring their online persona and checking their security settings

Pupils should not be signed up to most social networking sites due to the over-13 age limit. However, we recognise that many are signed up either with or without parental knowledge. As a school we will monitor the use of social networking and ensure it is part of our curriculum. We will also ensure that parents are fully aware of how to minimise the risk if their children are using these sites. As a school, we do reserve the right to contact sites such as Facebook and ask them to remove our children's accounts should any issues, such as cyber-bullying, occur.
As a school we will use Twitter to post information, updates and blog posts. These will stream directly to our school website. We will ensure that we block any followers that appear inappropriate.

Digital and Video Images

As a school, we will ensure that if we publish any photographs or videos of children online, we:

- Will ensure that their parents or guardians have given us written permission
- Will ensure if we do not have permission to use the image of a particular child, we will make them unrecognisable to ensure that they are not left out of situations unnecessarily
- Will not include a child's image and their name together without permission from the parents or guardians e.g. if the child has won an award
- Will ensure that children are in appropriate dress and we do not include images of children who are taking part in swimming activities
- Ask that if a parent, guardian or child wishes, they can request that a photograph is removed. This request can be made verbally or in writing to the child's teacher or to the computing coordinator. We will endeavour to remove the photograph as soon as possible
- Will provide new parents with a photo permission letter upon their arrival into school

- Will ask parents or guardians that are recording video or taking digital images at public events e.g. school play or sports day, that they do not publish these online.

Staff should not use personal cameras or phones to take photographs of children within school but instead use school iPads.

Complaints

Incidents regarding the misuse of the Internet by students will be delegated to the computing lead who will decide which additional evidence should be gathered or recorded. A partnership approach with parents will be encouraged. Any complaint about staff misuse will be referred to the Principal. Complaints of a child protection nature must be dealt with in accordance with child protection procedures, see Safeguarding policy.

Responding to unacceptable use by staff

Failure to comply with the guidelines and expectations set out for them could lead to sanctions being imposed on staff and possible disciplinary action being taken in accordance with the school's policy and possibly the law.

Responding to unacceptable use by pupils

Pupils should be aware that all E-Safety issues will be dealt with quickly and effectively. When dealing with unacceptable use, staff should follow the Behaviour Policy and if necessary, the Anti-bullying Policy. Children may have restrictions placed on their account for a short time.

Remote Learning

'Remote Learning' refers to the provision of work, teacher support, assessment and feedback from teachers to pupils in the event that normal lessons are unable to be delivered 'face-to-face' as normal.

Castleward Spencer Academy, is committed to providing continuity of education for its students in the event of an extended school closure. While such situations are inevitably highly varied in their causes and ramifications, we will endeavour to provide continued learning for our students during any period of closure in the following ways:

- Guidance of daily tasks on Class Dojo and via Purple Mash email
- Twice daily TEAMs calls as a class
- No 1:1s, groups only
- Staff and children must wear suitable clothing, as should anyone else in the household.
- Any computers used should be in appropriate areas, for example, not in bedrooms; and where possible be against a neutral background.

- Lessons will be pre-recorded and shared with families, so that learning can revisited as and when required.
- Live classes should be kept to a reasonable length of time, or the streaming may prevent the family 'getting on' with their day
- Language must be professional and appropriate, including any family members in the background
- Leaders will reassure themselves that any teaching/learning software and/or platforms are suitable and raise no privacy issues; or use cases against the providers terms and conditions (for example, no business use of consumer products)

Appendix 1

Acceptable Usage Forms

Acceptable Usage Policy Key Stage 2 Children

When we talk about computing, we are talking about computers, iPads and everything else including cameras and other devices. By using the computing equipment in school, you have agreed to follow these rules.

☺ At all times, I will think before I click (especially when deleting files)

☺When using the internet, I will think about the websites I am accessing

☺When using information or pictures from websites, I will try and say which website it came from and if possible link back to the site

☺ When communicating online (in blogs, email etc) I will think about the words that I use and will not use words that may offend other people

☺ When communicating online, I will only use my first name and not share personal details such as my email address or phone number

☺I know that the teachers can, and will, check the files and websites I have used

☺I will take care when using the computers and transporting equipment around

☺ I will keep my usernames and passwords secure, but I understand I can share them with appropriate people, such as my parents or teachers

☹ If I find a website or image that is inappropriate, I will tell my teacher straight away

☹ I understand that if I am acting inappropriately then my parents may be informed

☹ I understand that people online might not be who they say they are

☹ I will not logon using another person's account without their permission

Name:

Class:

Signed:

Date:

Acceptable Usage Policy Key Stage 1 Children

The Golden Rule: Think before you click

☺ I will be careful when going on the internet.

☺ I will only use the internet when a teacher is with me.

☺ I will tell a teacher if I see something that upsets me.

☺ I know people online might not be who they say they are.

☺ I will be polite when talking to people or writing online.

☺ I will think before I print or delete.

☺ I will be careful when using or carrying equipment.

☺ I will keep my password secret, but I can tell my family.

☺ I will remember to log off properly before closing the lid of the chrome book.

☹ I won't tell anyone any personal details like my phone number or last name.

☹ I won't logon using someone else's username.

☹ I won't put water bottles on the table when using computing equipment.

Name:

Class:

Signed:

Date:

Acceptable Usage Policy

This document has been written to ensure that staff use the computing throughout the school appropriately. If they have any questions regarding this policy, they should direct them to the Principal or the computing lead.

Staff should:

- Use computers and equipment with care and ensure children do the same e.g. water bottles should stay away from machines.
- Ensure that they have a sensible password.
- Ensure that usernames and passwords are not shared with children or other staff.
- Ensure that they log off when they have finished using a computer – particularly in shared areas.
- Ensure that online dialogue (e.g. blog posts or emails) with other schools, parents or children remains professional at all times.
- Ensure that online activity is related to their professional duty and that personal use should be kept to a minimum.
- Ensure that they are not using the school's computing for financial gain e.g. auction or betting sites.
- Be aware that software or hardware should not be installed without prior consent of the computing coordinator or Principal.
- Understand that inappropriate use of the school's network may result in some services being removed and further action being taken by the Principal.
- Where data of a personal nature such as school reports, IEPs, correspondence, photographs and assessment data is taken home on a school laptop or other storage device, it must be recognised that this data comes under the Data Protection Act and is subject to the school's Data Protection Policy. Care must therefore be taken to ensure its integrity and security. It must not be transferred to home computers and should be removed from any portable device including USB pens and memory cards as soon as is practical.
- Report any issues to the Principal or computing lead as soon as possible.
- Return any hardware or equipment if they are no longer employed by the school.

Signed _____ Print _____

Date _____

Acceptable Usage Policy Governors and Visitors

Visitors, both physical and virtual, may be provided with accounts to our network and/or online systems. Visitors will have a lower level of access than staff and each account will be provided on a case-by-case basis. This will depend on the purpose of the account requested.

Online Systems (Purple Mash, Google Apps, school website)

Visitors must provide the computing Coordinator with their name and email.
Users will:

- Not have access to mail or direct contact with children
- Understand that this account may be removed at any time so should not use it to save vital information

School Network and wireless

Users will:

- Be given a login for their time in the school
- Be expected to follow the guidelines as set out for staff
- Understand that this account may be removed at any time
- Be provided with the wireless key and guidelines for connecting to the network