CASTLE FARM

COUNTRYSIDE CLASSROOM

Acceptable Use of Technology Policy and Practice

09/24

Review date: 09/25

Company Number 14937009 Registered in England and Wales

CONTENTS

1 INTRODUCTION

2 RATIONALE

3 GENERAL STATEMENT

4 THE IMPORTANCE OF THE INTERNET AND MOBILE TECHNOLOGIES

5 IMPLEMENTATION AND PRACTICE SPECIFICALLY IN RELATION TO CHILDREN

- 5.1 Teaching About Online Safety: Underpinning Knowledge and Behaviours
  - *5.1.1 How to evaluate what they see online*
  - *5.1.2 How to Recognise Techniques Used for Persuasion*
  - *5.1.3 Online Behaviour*
  - *5.1.4 How to Identify Online Risks*
  - *5.1.5 How and When to Seek Support*
- 5.2 Managing the Risk Of Technology And Internet Access
- 5.3 Authorising Access
- 5.4 Managing E-Mail
- 5.5 Social Networking for Young People
- 5.6 Managing Other Forms Of Mobile Technology
- 5.7 Monitoring Safety and Security
- 5.8 Handling Complaints and Incidents
- 5.9 Communication and Responsible Use
- 5.10 Children's Involvement

6 IMPLEMENTATION AND PRACTICE SPECIFICALLY IN RELATION TO ADULTS

- 6.1 Unacceptable Behaviour
- 6.2 Company-Owned Information Held on Third-Party Websites
- 6.3 Electronic Communication Between Staff and Children
- 6.4 Social Networking Sites
- 6.5 Mobile Phones
- 6.6 Monitoring
- 6.7 Data Protection Responsibilities
- 6.8 Sanctions

7 SAFE WORKING PRACTICES

8 SOURCES OF ADDITIONAL INFORMATION

1 INTRODUCTION

We live in an age where technology and means of learning and communication through the use of technology are developing at an ever-increasing rate. Today's children 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. The Internet connects computers and technology worldwide and is used by millions of people. It is an invaluable source of information and communication that should be available for use by adults and children.

Children have the right to enjoy childhood online, to access safe online spaces, and to benefit from all the opportunities that a connected world can bring to them, appropriate to their age and stage. As they grow older, it is crucial that they learn to balance the benefits offered by technology with a critical awareness of their own and other's online behaviour and develop effective strategies for staying safe and making a positive contribution online.

2 RATIONALE

This document describes Castle Farm Countryside Classroom's policy and practice with respect to the use of technology, including the online world, and the publishing of its own website. The document should be read in conjunction with the Curriculum Intent Policy Statement, Computing Policy and Practice document, Safeguarding and Child Protection Policy, Relationships and Sex Education Policy and Anti-Bullying Policy all of which outline specific issues underpinning the approach at each establishment. Reference to the framework 'Education for a Connected World 2020' will ensure children are supported to understand age specific advice about online knowledge and skills.

This policy and practice document relates to both children and adults.

3 GENERAL STATEMENT

We believe that the educational and social benefits of Internet access, online communication, learning and connecting through technology and the publishing of our own website far outweighs the possible risks involved, and that good planning and careful management will ensure appropriate and effective child use. Internet access is available to both children and staff and therefore this document refers to both.

Home Internet use has rapidly expanded, in parallel with the continued growth of mobile technologies, and has become an important part of learning and communication during education and leisure time. The Internet is managed by a

worldwide collaboration of independent agencies that serve to attract a range of audiences and 'customers'. Without appropriate measures, access to unsuitable materials would be possible and security compromised. Equally by publishing our own website, access is possible for anybody in the world via the Internet. Therefore appropriate measures must be employed to protect individuals in terms of privacy and exploitation.

4 THE IMPORTANCE OF THE INTERNET AND MOBILE TECHNOLOGIES

The purpose of internet access at CFCC is educational, social, cultural and managerial. Mobile technologies (3G/4G/5G) have expanded opportunities for both children and staff to access, interact and communicate educationally and socially using an increasing number of devices.

Access to the Internet is a necessary tool for staff and an entitlement for children who show a responsible and mature approach. It should be noted that the use of a computer system without permission or for a purpose not agreed by the establishment could constitute a criminal offence under the Computer Misuse Act 1990.

A number of studies and government projects have indicated the benefits to be gained through the appropriate use of the Internet in educational, social and cultural terms. These benefits include:

- Access to world-wide educational resources, e.g. museums and art galleries
- Information and cultural exchanges between children world-wide.
- News and current events.
- Cultural, social and leisure use in libraries, clubs and at home.
- Discussion with experts in many fields for children and staff.
- Staff professional development - access to educational materials and good curriculum practice, access to social work research and practice documents, access to up to the minute research in the health field.
- Communication with external advisory and support personnel, professional associations and colleagues.
- Exchange of administration data with outside bodies.
- Preparation for children for the world they live in.
- Entrepreneurial opportunities.

5 IMPLEMENTATION AND PRACTICE SPECIFICALLY IN RELATION TO CHILDREN

5.1 TEACHING ABOUT ONLINE SAFETY**:** UNDERPINNING KNOWLEDGE AND BEHAVIOURS

As the online word develops and changes at a great speed it is important to focus on the underpinning knowledge and behaviours that can help children to navigate the online world safely and confidently regardless of the device, platform or app. To support this we may undertake focused interventions. Teaching and learning must always be age and developmentally appropriate, informed by the key adults specific

knowledge of the young person as well as the information provided by the 'Education for a Connected World 2020' framework.

Children will be encouraged to tell a member of staff immediately if they encounter any material that makes them feel uncomfortable. This includes situations of peer on peer abuse, cyberbullying or the sharing of nudes or semi nudes (see Sharing of Nudes and Semi-Nudes: advice for education settings working with children and young people and Castle Farm Countryside Classroom's Safeguarding and Child Protection Policy and Practice Document).

The following knowledge and behaviours will be included:

5.1.1 How to evaluate what they see online

This will enable children to make judgements about what they see online and not automatically assume that what they see is true, valid or acceptable. For example:

- Is this website/URL/email fake?
- How can I tell?
- What does this cookie do and what information am I sharing?
- Is this person who they say they are?
- Why does someone want me to see this?
- Why does someone want me to send this?
- Why would someone want me to believe this?
- Why does this person want my personal information?
- What's behind this post?
- Is this too good to be true?
- Is this fact or opinion?

5.1.2 How to Recognise Techniques Used for Persuasion

This will enable children to recognise the techniques that are often used to persuade or manipulate others. Understanding that a strong grasp of knowledge across many areas makes people less vulnerable to these techniques and better equipped to recognise and respond appropriately to strongly biased intent or malicious activity. We can help children to recognise:

- Online content which tries to make people believe something false is true and/or mislead (misinformation and disinformation).
- Techniques that company use to persuade people to buy something.
- Ways in which games and social media companies try to keep users online longer (persuasive/sticky design).
- Criminal activities such as grooming.

5.1.3 Online Behaviour

This will enable children to understand what acceptable and unacceptable online behaviour look like. CFCC should teach children that the same standard of behaviour and honesty apply on and offline, including the importance of respect for others. CFCC should also teach children to recognise unacceptable behaviour in others. CFCC can help children to recognise acceptable and unacceptable behaviour by:

- Looking at why people behave differently online, for example how anonymity (you do not know me) and invisibility (you cannot see me) affect what people do.
- Looking at how online emotions can be intensified resulting in mob mentality.
- Teaching techniques (relevant on and offline). to defuse or calm arguments, for example a disagreement with friends, and disengage from unwanted contact or content online.
- Considering unacceptable online behaviours often passed off as so-called social norms or just banter. For example, negative language that can be used, and in some cases is often expected, as part of online gaming and the acceptance of misogynistic, homophobic and racist language that would never be tolerated offline.

5.1.4 How to Identify Online Risks

This will enable children to identify possible online risks and make informed decisions about how to act. This should not be about providing a list of what not to do online. The focus should be to help children assess a situation, think through the consequences of acting in different ways and decide on the best course of action. CFCC can help children to identify and manage risk by:

- Discussing the ways in which someone may put themselves at risk online.
- Discussing risks posed by another person's online behaviour.
- Discussing when risk taking can be positive and negative,
- Discussing "online reputation" and the positive and negative aspects of an online digital footprint. This could include longer-term considerations, i.e. how past online behaviours could impact on their future, when applying for a place at university or a job for example.
- Discussing the risks vs the benefits of sharing information online and how to make a judgement about when and how to share and who to share with.
- Asking questions such as what might happen if I post something online? Who will see it? Who might they send it to?

5.1.5 How and When to Seek Support

This will enable children to understand safe ways in which to seek support if they are concerned or upset by something they have seen online. CFCC can help children by:

- Helping them to identify who trusted adults are (at CFCC this could be any adult whom they have built a trusting relationship.
- Looking at the different ways to access support from CFCC, police, the National Crime Agency's Click CEOP reporting service for children and 3rd sector organisations such as Childline and Internet Watch Foundation (The CFCC Safeguarding and Child Protection policy and processes around reporting of safeguarding and child protection incidents and concerns to staff should be applied).

- Helping them to understand that various platforms and apps will have ways in which inappropriate contact or content can be reported.

5.2 MANAGING THE RISK OF TECHNOLOGY AND INTERNET ACCESS

In common with other media such as magazines, books and video, some material available via technology and the Internet is unsuitable for children. CFCC will advise and support children and take all reasonable precautions to ensure that users access only appropriate material. CFCC cannot accept liability for the material accessed, or any consequences thereof.

- Methods to quantify and minimise the risk will be reviewed formally, and remain under continual scrutiny in liaison with the ISP.
- Staff will check that the sites selected for child use are appropriate to the age and maturity of children.
- CFCC, its staff, parents, placing authorities and external advisers will work to establish agreement that every reasonable measure is being taken.
- The CFCC Directors will ensure that this policy is implemented effectively.
- CFCC Directors will act as the lead professional for e-safety related concerns and issues.
- Each child will have an IT related section within their individual Risk Assessments
- New technologies are embraced as a potential learning opportunity but assessed for risk on an ongoing basis.

5.3 AUTHORISING ACCESS

- Parents will be informed that children will be provided with Internet access where it is important to support their learning

5.4 MANAGING E - MAIL

- Communications with persons and organisations will be managed to ensure appropriate use and that the good name of CFCC is maintained.

5.5 SOCIAL NETWORKING FOR YOUNG PEOPLE

- Social networking sites are not accessed during the learning activities at Castle Farm.

5.6 MANAGING OTHER FORMS OF MOBILE TECHNOLOGY

- Children may be allowed mobile phones on site but these decisions will be monitored through individual risk assessment.

5.7 HANDLING COMPLAINTS AND INCIDENTS

- Responsibility for handling complaints and incidents will be given to the Directors
- Children and parents/carers will be informed of the procedure.
- Parents/carers and children will need to work in partnership with staff to resolve any issue.
- As with other issues, there may be occasions when the police must be contacted. Early contact will be made to establish the legal position and discuss strategies.
- If staff or children discover unsuitable sites, the URL (address) and content will be reported to the Service Provider.

The CFCC Safeguarding and Child Protection Policy should be read when dealing with technology related incidents.

5.9 COMMUNICATION AND RESPONSIBLE USE

- Rules for Internet access and responsible use will be made clear to individuals and groups.
- All staff will have access to the Acceptable and Safe Use of Technology Policy, and its importance explained.
- Children, schools, parents' and placing authorities attention will be drawn to the Policy via the admission process.
- Staff will assist, where applicable, parents/carers to develop a well informed and balanced view of the risks and benefits.

IMPLEMENTATION AND PRACTICE SPECIFICALLY IN RELATION TO ADULTS

Use of the Internet and technology by employees of Castle Farm Countryside Classroom is permitted and encouraged where such use supports the goals and objectives of the business.

However, CFCC has a policy for the use of the Internet and technology whereby employees must ensure that they:

- comply with current legislation;
- use the internet, technology and social media in an acceptable way;
- do not create unnecessary business risk to the company by their misuse of the internet, technology or social media.

Safeguarding training supports adults to understand the breadth of issues classified within online safety, categorised into four areas of risk:

- Content - being exposed to illegal, inappropriate or harmful content; for example, pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.
- Contact - being subjected to harmful online interaction with other users; for example, 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; for example, 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; and
- Commerce - risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your children, students or staff are at risk, please report it to the Anti-Phishing Working Group.

6.1 UNACCEPTABLE BEHAVIOUR

In particular the following is deemed unacceptable use or behaviour by employees:

- visiting internet sites that contain obscene, hateful, pornographic or otherwise illegal material.
- using the computer or device to perpetrate any form of fraud, or software, film or music piracy.
- using the internet to send offensive or harassing material to other users.
- downloading commercial software or any copyrighted materials belonging to third parties, unless this download is covered or permitted under a commercial agreement or other such licence.
- hacking into unauthorised areas.

6.2 COMPANY-OWNED INFORMATION HELD ON THIRD-PARTY WEBSITES

If you produce, collect and/or process business-related information in the course of your work, the information remains the property of CFCC This includes such information stored on third-party websites such as webmail service providers and social networking sites, such as Facebook and LinkedIn.

6.3 ELECTRONIC COMMUNICATION BETWEEN STAFF AND CHILDREN

The CFCC Directors must approve any proposed electronic communication with children. This applies to many potential areas, and includes social networking, mobile phones, online gaming and personal email.

ONEDRIVE

CCFCC uses Microsoft OneDrive, which is a file hosting service operated by Microsoft. First released in August 2007, it allows registered users to store, share and sync their files. We currently use this platform to securely share relevant information on staff and students, such as preadmission paperwork, risk assessments etc. This platform can be accessed via computers, mobile phones, tablets etc. The password for this must be kept confidential and changed should an

employee leave our employment. This service is constantly overseen by directors and any additions to the onedrive must completed by directors only.

For children attending CFCC:

- Staff should not provide their personal mobile phone number; any calls required to a child should be made using the 141 prefix to protect their details.
- Web based email addresses should not be shared between children and staff.
- There should be no direct connections on any form of social media or through chatrooms within online games between staff and children.
- Parents are given staff contact numbers where necessary, to allow communication with specific tasks such as transport arrangements. This is done with the agreement of all parties.

6.4 SOCIAL NETWORKING SITES

Staff need to be aware of the dangers, boundaries and limitations in terms of how something said, either in person, or online, may be interpreted by others. Social networking sites are no different than any other social setting and staff should be aware of how they represent themselves and the company in any form of conversation.

6.5 MOBILE PHONES

All staff should have a mobile phone available whilst at work to maintain contact with the provision and when engaging with children and young people on activities. However, the use of a mobile phone is potentially a sensitive issue; it can be both helpful and engaging as a learning tool, whilst also presenting as a clear rejection to a child. For example, if a child is with a staff member who diverts their attention to their phone, whether to take a call, receive or send a message or simply to browse the internet, the child will potentially feel secondary to the device. This would be the same as ignoring a child or turning attention to another person. All staff must recognise the importance of role modelling socially acceptable behaviour in these situations.

When engaging in activities with children or young people, staff may wish to capture images on their phone for use with student daily uodates. It is essential these are downloaded at the earliest opportunity and the original images or video deleted

from their device and any cloud backups. Contravention of this guidance could lead to the adult being subject to the company's disciplinary procedure.

6.6 MONITORING

CFCC accepts that the use of the Internet is a valuable business tool. However, misuse of this facility can have a negative impact upon employee morale and the reputation of the business.

6.7 DATA PROTECTION RESPONSIBILITIES

Staff are responsible for adhering to the principles of the General Data Protection Regulation that are defined in the CFCC Data Protection Policy and Practice document. Staff must ensure they follow the guidance for processing both their own and others personal information, with reference to the CFCC Data Protection policy and Practice document section 6 (Staff Responsibilities). In particular:

- Any personal data that you hold is kept securely.
- Personal information is not disclosed either orally or in writing, accidentally or otherwise to any unauthorised third party.
- Personal information is not transferred internationally without checking first that the right safeguards are in place.
- You avoid leaving any portable or mobile ICT equipment or removable storage media in unattended vehicles. Where this is not possible, it must be locked out of sight.
- Passwords and login information are not disclosed to anyone else.
- Personal information is kept in a locked filing cabinet, or in a locked drawer, or if it is computerised, be password protected.
- If kept temporarily on portable media personal information must be password protected, encrypted and kept securely, having been first discussed with the data manager.

Adhering to the procedures outlined in the ‘Maintaining Security’ section below is essential to reduce the potential risk of a data breach of personal data relating to the children or the adults.

6.8 SANCTIONS

Where it is believed that an employee has failed to comply with this policy, they will be subject to the company's disciplinary procedure. If an employee is found to have breached the policy, this will result in disciplinary action and possibly dismissal.

7 Safe Working Practices

- If an adult needs to leave their computer or device unattended as a temporary measure whilst working, the screen saver (display lock) should be activated.
- If data is to be transferred on any form of portable media, this must be first discussed with a Director and be fully encrypted.
- We do not store digital media of CFCC children. Photos are shared with the referring party at the earliest opportunity and not kept on company laptops or other forms of technological devices once transferred from the source device.
- All laptops issued by CFCC to staff will have encrypted hard drive back ups wherever possible.
- Staff may communicate between groups using WhatsApp. Directors act as admin for these created groups to ensure that correct procedures are adhered to.

Video conferencing and calls

- Meetings may be conducted through virtual means such as Zoom or Teams. In these circumstances staff must maintain confidentiality and consider the environment in which they participate in the meeting. For example, the potential to be overheard in a public setting or even within a shared home must be considered.

8 SOURCES OF ADDITIONAL INFORMATION AND SUPPORT

- Education for a Connected world
- Teaching Online Safety in Schools 2017
- Sharing Nudes and Semi-Nudes: Advice for Education Settings December 2020
- Keeping Children Safe in Education – Annex D (Online Safety)

.