ST. CHAD'S CATHOLIC PRIMARY SCHOOL

*At St Chad's we are part of Gods family. *We learn from Jesus' teachings in the Gospel *We love Jesus and love each other with all our hearts *We show kindness to everyone just like Jesus did.*

EYFS DIGITAL MEDIA POLICY

Date of review: March 2022

Date of next review: March 2024

Reviewed by: Krystyna Bickley

Date of Governing Board ratification:23rd March 2022

Introduction

This policy provides guidance and practical advice to staff and volunteers in safeguarding children from the possible risks associated with digital technology as well as ensuring that staff protect themselves through safe and responsible working practices.

New technologies open up many exciting benefits and opportunities for learning and development but can also present risks. Wider access to technology via iPads/tablets, mobile phones, games consoles and other devices bring new challenges about controlling access and content.

Although children within Early Years Settings will not normally be accessing technology independently and benefit from a high level of supervision, there is always a small element of risk.
Safeguarding is everyone's responsibility and all providers have a role in helping children stay safe on line and supporting the adults who work with children in minimising risks.

The value of IT as a learning tool is embedded within the Early Years Foundation Stage. Early years practitioners and managers should therefore support children and young people in using a range of IT (resources) which may include cameras, photocopiers, recording devices and programmable toys in addition to computers.

Early Years practitioners and their managers should also be able to support children and young people to talk about IT apparatus, what it does, what they can do with it and how to use it safely. It is also important for parents and carers to be fully involved with promoting online safety within the setting, home and social environment.

E safety responsibilities for providers include technological infrastructure, filtering and monitoring systems, recognition and responses to e safety concerns plus ongoing risk assessment to identify emerging issues.

Safer Working Practice is essential as although most people who work with children have their best interests at heart, we know that sadly some people have abused their position of trust to abuse children in ways that have been further amplified through the digital environment. This should therefore be seen as part of the broader responsibilities that everyone working with children has to safeguard their welfare.

Photography and Videos

IT has an important role in supporting children's learning and development. For example, photographs of children engaged in a variety of activities and experiences can provide valuable evidence to include within learning journals.

To promote safer use of IT, it is essential that when work with children involves the taking or recording of images this should safeguard the privacy, dignity and well-being of children. Informed written consent should be obtained from parents or carers and agreement should also be sought from the child, where possible.

Care should be taken to ensure that all parties understand the implications especially if the image is to be used for any publicity purposes or published in the media. There should be agreement as to how the images will be stored, and for how long. Adults need to be sensitive to children who appear uncomfortable and be alert to the potential for such activities to lead to misunderstandings. It is not appropriate for adults to take photographs of children for their own personal use.

Helpful Hints

Do

- Be clear about the purpose of the activity and what will happen to the images
- Be able to justify images of children in your possession
- Avoid making images in one to one situations or that show a single child with no surrounding context
- Ensure the child understands why the images are being taken and that they are appropriately dressed
- Only use equipment provided or authorised by the organisation
- Report any concerns about inappropriate or intrusive images found
- Ensure you have parental permission to take and/or display photographs

Do Not

- Display or distribute images without consent
- Use images that could cause distress
- Use personal mobile phones or other personal devices to take photographs.
- Take images ‘in secret’ or images in situations that could be construed as being secretive

Closed Circuit Television (CCTV)

Using CCTV can help in monitoring and security both within the setting and around the external site. When using CCTV school should observe the following

Do

- Ensure areas covered by CCTV are clearly signposted
- Ensure the manufacturer’s instructions and data protection guidelines are followed at all times. This should include appropriate storage and disposal of all recordings
- Recordings should be retained for a limited time period and no longer than their intended purpose. Generally, this is no longer than 30 days. Recordings should be erased before disposal including recordings taken outside of operational hours
- Regular auditing of stored images should be undertaken by the lead practitioner or designated senior leaders.
- Ensure sensitive positioning of cameras to avoid inadvertently taking inappropriate images. Cameras should not be pointed directly at toilet cubicles or other sensitive areas
- Where images recorded give cause for concern or involve criminal activity, the information should be referred to the relevant agency

Access to Inappropriate Images and Internet Use

In the Early Years the use of internet enabled devices, including iPad educational apps and games, are used to enhance the learning experience of children or as online tools for staff to track and share achievement. For this reason, great care must be taken to ensure that safe and secure internet access, appropriate for both adults and children, is made available regardless of the size of the setting.

There are no circumstances that will justify adults possessing indecent images of children. Accessing, making and storing indecent images of children on the internet are illegal. Adults who are involved in this activity will be viewed as a threat to children and will be subject to a criminal investigation that if proven will result in them being barred from working with children.

- Adults should not use equipment belonging to the setting to access pornography, nor should personal equipment containing such images be brought into the workplace.
- Adults should ensure that children are not exposed to inappropriate images or web sites.

Appropriate controls should be in place to prevent this, for example, through use of filters and personal passwords. In larger settings age appropriate content filtering must be in place across the setting, ensuring that staff and children receive different levels of filtered internet access in line with user requirements (e.g. You tube at staff level but blocked to children)

School staff must ensure that parental controls are established on all internet enabled devices that children have access to, blocking or preventing access to any harmful, illegal or inappropriate content.

Where indecent images are found, this must be reported immediately via the manager (unless the manager is the subject of the concern) who will alert the Police and/or the Local Authority Designated Officer (LADO).

Adults who discover such images should not attempt to investigate the matter themselves as this could compromise an investigation

Do

- Have policies in place about internet use for example through an acceptable use agreement
- Follow guidance on the use of IT equipment
- Ensure that children are not exposed to unsuitable material on line
- Ensure that any films, games or material shown to children and young people are age appropriate

Communication with Children through technology

Communication between children and adults should take place within clear and explicit professional boundaries. This includes the use of technology such as mobile phones, text messaging, websites etc. Adults should ensure that all communications are transparent and open to scrutiny. There is a need to be cautious to avoid any possible misinterpretation of motives or behaviour that could be interpreted as grooming. Adults should not therefore give personal contact details to children unless in exceptional circumstances the need to do so is agreed with staff and parents. E mail communications should be professional in tone and content and e mail systems should be used in accordance with the acceptable use agreed policy.

Do

- Have an agreement about permissible and acceptable modes of communication
- Only use equipment provided by the setting to communicate with parents/children
- Only make contact with children for professional reasons and follow acceptable use agreement

Do Not

- Give out personal contact details to children or young people
- Use internet or web-based communication channels to send personal messages to a child or young person

Use of Social Networking Sites

Social networking sites (e.g. Facebook and Twitter) can be a useful advertising tool for early year's settings and can often be an effective way of engaging with parents. Due to the public nature of social networking and the inability to keep content truly private, great care must be taken in the management and use of such sites. Best practice guidance states that:

- Identifiable images of children should not be used on social networking sites.
- To maintain professional distance and to avoid unwanted contact, staff should not link their personal social networking accounts to the setting's page.
- Ensure that privacy settings are set to maximum and checked regularly.
- For safeguarding purposes, photographs or videos of looked after children must not be shared on social networking sites.

Staff should ensure that their personal use of social media does not conflict with their professional role and be mindful of information they post on line. Staff should observe confidentiality and not discuss issues relating to work on line or bring the setting into disrepute. Privacy settings should be set to block unauthorised access to the account and staff should avoid accepting children and parents as 'friends' as this can compromise professional boundaries.

Applications for recording children's progress

In recent years, a number of applications (apps) for mobile devices have been launched which are targeted specifically at Early Years Practitioners and settings. Many of these apps allow staff to track and share a child's learning journey online with parents and carers, usually in the form of photographs and text. Such tools have considerable benefits, including improved levels of engagement with parents and a reduction in paperwork, but careful consideration must be given to safeguarding and data security principles before using such tools.

- Personal staff mobile phones or devices (e.g. iPad or iPhone) should not be used for any apps which record and store children's personal details, attainment or photographs. Only setting issued devices may be used for such activities, ensuring that any devices used are appropriately encrypted if taken off site. This is to prevent a data security breach in the event of loss or theft.
- Before purchasing or accessing any apps for staff or children's use, senior leaders must have a clear understanding of where and how children's data will be stored, including who has access to it and any safeguarding implications.
- Please note: The senior leaders and governors are ultimately responsible for the security of any data or images held of children within the setting.

Data Protection

Data Protection means that all who hold personal data either on paper or electronically must keep it secure.

Personal data is defined as any data that enables an individual to be identified including names, contact details, and so on.

Any item that can hold information requires controls to be put in place to prevent it being damaged or stolen. This will include CDs, DVDs and memory sticks. Sensitive data, photographs and videos of children should not be stored on setting devices which leave the premises (e.g. laptops, mobile phones, iPads, USB Memory Sticks etc) unless encryption software is in place.
All staff should be aware of the settings guidance regarding storage, transmission and removal to ensure data is kept safe.

Responding to Concerns

Any concern in a child care setting should in the first instance be reported to the EYFS Lead Practitioner, (unless they are the subject of concern) in which case seek advice from the Principal or Local Authority Designated Officer
The Principal will consider whether the concern needs to be referred to The Police and/or Children's Social Care as a safeguarding incident. If the concern is about the behaviour of staff or volunteers then it should be reported to the Local Authority Designated Officer.

This policy should be read in conjunction with the Safeguarding and Child Protection policy.