TECHNOLOGY AND ONLINE SAFETY POLICY AND PROCEDURES

Approved by: SMT

Approved date: September 2021

To be reviewed by: SMT

Review date: September 2022

Accessibility: Available on the school website and as paper copy on request

Scope: Ashbridge Independent School and Nursery, Ashbridge-on-Ribble Nursery, Ashbridge Nursery at Maxy Farm, The Fledglings Nursery

*In the context of this policy "everyone" refers to Employees, freelance teachers, supply staff, students, volunteers, contractors and anyone else working for or on behalf of Ashbridge School Ltd.

INTRODUCTION

It is vital that our staff and children are sufficiently educated and know the policies and procedures to follow when working online or using technology. We also ensure we inform, communicate with and educate parents and carers about online safety.

This policy is to be used together with the Personal Development Programme, Computing Policy and Scheme of Work, Safeguarding and Child Protection Policy and Procedures, Remote Learning Policy, Anti-Bullying Strategy, Behaviour Policy and the Acceptable Use Policies: "Children in School", "Staff" and "Directors, Students, Freelance Teachers, Volunteers etc".

The policy is split into three sections relating to the online conduct and requirements for children, parents and staff. It is essential that staff members read and understand all three sections.

STAFF ROLES AND RESPONSIBILITIES

The school's Lead Person for Online Safety is Director of Compliance, Charlotte Bingham Brindle. It is their responsibility, together with the rest of the SLT and DSLs, to ensure all staff have access to regular professional development related to online safety and make sure pupils are receiving suitable education and guidance. The Lead Person for Online Safety is also responsible, together with the ICT technician, to ensure the school's technology provide a safe and secure online environment for all staff and children. All staff also have a duty to ensure the children are able to work and learn in a safe and secure online environment.

CHILDREN

SAFEGUARDING CONCERNS

Keeping children safe online and providing them with the tools to stay safe online when out of school is of utmost importance. By focussing on the 4Cs of online safety; content, contact, context and commerce, we can ensure that we are doing all we can to protect children online.

Content

Managing the content children see online is vital to ensure they are not exposed to illegal, age-inappropriate or otherwise harmful material including, but not limited to; pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism. In school we do this by using a filtering system that protects from this type of content without unreasonable blocking of websites. A children's search engine, Kiddle, and other safeguarding systems are also in place where required. The Personal Development Programme (PDP) and Computing curriculum also teaches children how to manage the content they see and what to do if they come across inappropriate content.

Contact

The systems we have in place ensure children are not subjected to harmful online interaction with others, such as peer pressure, unsuitable commercial advertising or adults posing as children with the intention to groom or exploit them. We do this by not allowing mobile devices or smartwatches with internet connectivity in school at any time and providing teaching through the PDP and Computing programme.

Conduct

A key skill for children to learn is how to conduct themselves online by learning how to avoid acting in a way that increases the likelihood of, or causes, harm. Examples of inappropriate conduct online includes, but is not limited to; making, sending and receiving of explicit images, online bullying and 'trolling'. We do this through the PDP and Computing programme and with activities on Safer Internet Day.

Commerce

*In the context of this policy "everyone" refers to Employees, freelance teachers, supply staff, students, volunteers, contractors and anyone else working for or on behalf of Ashbridge School Ltd.

Our filtering systems ensure that children cannot access inappropriate commerce materials such as online gambling, phishing, scams or inappropriate advertising. Through the PDP and Computing programme children learn about different types of scams, phishing and how to exercise caution when clicking on links when online.

The filtering and monitoring systems are managed by the ICT technician and it is everyone's responsibility to report to him or Charlotte Bingham Brindle if they find material that is harmful or inappropriate, or if they are unable to access a website they require for teaching, learning, monitoring or assessment purposes.

If children are required to undertake remote learning, safe, approved platforms including Microsoft Teams, Zoom and Seesaw are used and clear policies and procedures are in place as detailed in our Remote Learning policy.

Regular staff training, staff vigilance and appropriate filtering systems mean we do all we reasonably can to limit children's exposure to online risks. Youth-produced sexual imagery

CYBER-BULLYING

Cyber-bullying is a serious and ever-changing problem and it is vital that we protect our children at Ashbridge, help them to build resilience and learn how to protect themselves online through our safeguarding procedures and education. Cyber-bullying can take many forms which may include, but are not exclusively: offensive messages, phone calls or other communications; posting inappropriate photographs or videos of others; making offensive or threatening comments about others on social media, group chats or any other form of digital communication; exclusion, abuse or excessive targeting in online gaming; and hacking social network or email accounts.

Though the PDP programme, Computing curriculum, Safer Internet Day and other teaching we encourage children to act responsibly online and report any concerns to a parents or trusted adult at school. Any incidents of cyber-bullying will be managed as detailed in the behaviour policy.

SOCIAL MEDIA AND GAMING

Whilst we educate parents and children about the legal ages for social media platforms and gaming we recognise that some children do have social media accounts or access age-inappropriate games out of school and we do all that is reasonably practical to discourage this and educate children and parents in the safe use of social media and age-appropriate gaming. Through the Personal Development Programme (PDP) children discuss the impacts of social media and gaming, both positive and negative.

Social media is an incredibly useful tool for communication and marketing and it is important that members of the Ashbridge team use social networks in a responsible and appropriate manner. Misuse of social media platforms can have a damaging impact on both individuals and the company as a whole. Director of Compliance, Charlotte Bingham Brindle, and Director of Operations, Grace Cole, oversee all company social media engagement, with Grace Cole having specific responsibility for Twitter and Charlotte Bingham Brindle having specific responsibility for Facebook and Instagram.

USE OF MOBILE DEVICES

Children in school, nursery or Holiday Care are not permitted to use any mobile devices whilst in school or nursery except those provided by the school and nursery, and such devices must not be brought onto the premises. This includes mobile phones, tablets, smart watches, portable games consoles and any other electronic device

*In the context of this policy "everyone" refers to Employees, freelance teachers, supply staff, students, volunteers, contractors and anyone else working for or on behalf of Ashbridge School Ltd.

PARENTS, CARERS AND OTHER FAMILY MEMBERS

SOCIAL MEDIA

If parents have any queries, concerns or complaints about the school or nursery these should be raised with the school directly and not through social media platforms. This includes direct messaging on the school's social media accounts or messaging members of staff individually. Company social media accounts are only monitored during working hours Monday-Friday.

If any parent or other family member of a child is found to have posted or shared anything about the company or staff which is malicious, inappropriate or defamatory on any social media platform it is likely they will be asked into school or nursery for a meeting and be asked to remove the content in order to resolve the issue.

Parents are asked to refrain from requesting friendship of staff members or follow any personal accounts of staff on social media to protect their privacy.

MOBILE DEVICES

All customers and visitors are made aware that the use of mobile devices, including smartphones, whilst on the school and nursery premises is prohibited, unless in one of our 'Mobile Phone Zones'. Signage is placed in all prominent areas to this effect and is agreed within the Welcome Pack.

Parents/carers and visitors are not permitted to use any recording device or camera, including those on a mobile phone, on the premises without prior consent from the management team, and are made aware of this at the time of enrolment.

During special events such as performances we may allow parents to take photographs or video recordings with permission on the understanding that these will be used for personal use only, as set out in the School and Nursery Parent Handbook.

USE OF CAMERAS AND PHOTOGRAPHS

Within school and nursery, photographs video recordings are taken to be used as:

- Records and evidence of individual children's learning and experiences
- Teaching materials
- Records of activities and events
- For display, publications and promotional and marketing purposes both in print and online by the school and local or national media outlets.

Written permission to take and use photographs and videos of children is requested from parents/guardians at the time of enrolment. This includes use of the child's photographs or videos once they have left Ashbridge and permission for using images on our tracking software. If permission is not given for one or more of these uses, then we respect and adhere to this. Where relevant, we find alternative ways of recording children's learning. Staff are made aware of photo and video permission requests by referring to lists which are issued to each Room Leader and class teachers. Parents/guardians are given the option to change their child's permissions on an annual update form, or can contact the school or nursery at any time.

When professional media companies or photographers are commissioned or members of the press come to take pictures or videos for promotional purposes they too work within company guidelines and are supervised whilst

*In the context of this policy "everyone" refers to Employees, freelance teachers, supply staff, students, volunteers, contractors and anyone else working for or on behalf of Ashbridge School Ltd.

on the premises. A commercial company is also used to take individual and group photographs of children for purchase by parents/guardians on approximately two occasions each year. These sessions and the procedures for management and distribution are supervised by the management team and photographers are aware of their responsibilities and are required to act within company guidelines also.

EMPLOYEES, FREELANCE TEACHERS, SUPPLY STAFF, STUDENTS, VOLUNTEERS AND CONTRACTORS

SOCIAL MEDIA

Everyone* at Ashbridge has a responsibility to ensure that their use of social media platforms, both in and out of work promotes the company in a positive way and upholds the Ashbridge reputation. It is important that the company or those who work for the company are not displayed in a negative way on any social media or messaging services; such as Whatsapp, Facebook, TikTok, Twitter, Instagram, Snapchat, YouTube or any other website that involves sharing personal information. Safeguarding children is a key responsibility of all members of staff and it is essential that everyone considers this and acts responsibly if they are using social media sites. **Anyone working at Ashbridge either as a paid employee or volunteer must not communicate with children or parents via personal social media accounts or other messaging services, and should exercise caution when communicating with each other.** An exception to this would be when parents are already friends with team members outside of the work setting, although team members should not discuss work matters with friends who are also parents of children at Ashbridge. If a member of the team is in any doubt about whether an online friendship is appropriate they should discuss this with their line manager or Charlotte Bingham Brindle.

Sharing of information or data about children, parents or staff members in social media groups, including WhatsApp or Messenger is not acceptable and caution should be exercised when sharing information between individuals. It is essential that children or other adults are not identifiable from one-to-one conversations over social media.

Code of Conduct – Social Media

The following are **not acceptable**:

1. The use of the company's name, logo, or any other published material without written prior permission from the SLT. This applies to any published material on the internet or written documentation.
2. The posting, sharing or commenting by anyone of any communication or images/videos which links employees, students or volunteers of the school and nursery to any form of illegal conduct or conduct which may damage the reputation of the company. This includes defamatory comments.
3. The disclosure of confidential or business-sensitive information; or the disclosure of information or images that could compromise the security of the company.
4. The posting of any images/videos on personal accounts of employees, children, parents, directors or anyone directly connected with the company whilst engaged in school/nursery activities.
5. The posting of out-of-work activities whilst still wearing Ashbridge uniform or branded items.
6. Being 'friends' with customers on social networks, unless the friendship has formed outside the workplace and not as a result purely of being linked through the child.
7. The sharing of data or information relating to a child, parent or member of staff in social media groups.

Specific Guidelines Relating to Posting on Company Twitter and Instagram Accounts

*In the context of this policy "everyone" refers to Employees, freelance teachers, supply staff, students, volunteers, contractors and anyone else working for or on behalf of Ashbridge School Ltd.

Twitter and Instagram are tools that we use at Ashbridge to promote the company and communicate with parents and it is essential that all members of staff are aware of the requirements when using Twitter or Instagram.

1. Staff must not use their personal accounts for school and nursery business. On Twitter, each area should have an account in nursery and each class in school eg:- @ashbridgebabies or @ashbridgeyear6. There is currently one Instagram account: @ashbridgeoutdoors
2. Photos and videos shared on Twitter and Instagram must show children in a positive manner and follow the guidelines detailed in the "Use of Cameras, Photographs and Videos" section of this policy.
3. The names of children should not be included on any picture or video shared on Twitter or Instagram.
4. Any photos or articles that are 're-tweeted' or shared from individuals or companies must also follow the photo guidelines and be in line with the values of our company.
5. Hashtags used must be appropriate and relevant to the content being tweeted.

Potential and Actual Breaches of the Code of Conduct

Regular monitoring is carried out by Director of Operations, Grace Cole and Director of Compliance, Charlotte Bingham Brindle. In instances where there has been a breach of the above Code of Conduct, the following will apply:

- Any breaches of this policy will be fully investigated. Where it is found that there has been a breach of the policy this may result in action being taken under the Disciplinary Procedure.
- The company will take appropriate action in order to protect the company reputation and that of its staff, parents and children and anyone else directly linked to Ashbridge School Ltd.

In the case of a child's activity on social media being deemed unsuitable, the Behaviour Policy will apply, referring also to the signed Acceptable Use Policy.

USE OF MOBILE DEVICES

The term 'mobile devices' refers to smart phones, tablets, smart watches or any other portable device with the capability of connecting to the internet or sending communications.

Personal Mobile Devices

1. Employees must not use personal mobile devices in any classroom or in any area designated for children. The only exception to this rule is when team members are in the forest or away on trips. Managers may also carry their phones in the case of Lockdown or fire evacuations.
2. Employees take their own mobile phones into the forest or on trips for communication with school and emergencies only. Employees are not permitted, under any circumstances, to use their own devices for personal use or taking photographs/videos at any time when they are with children.
3. Employees, excluding members of the Senior Leadership Team, should not use personal mobile phones for business purposes, unless in an emergency when there is no other option. Personal calls should be made in a discreet fashion and away from all areas designated for children's use, for example in the staff room or in an office area, behind closed doors.
4. Employees are not permitted to use the schools Wi-Fi on their personal mobile devices without specific permission from the SLT.
5. Employees must not take or store photographs/videos of children or store contact details of parents or guardians on personal mobile devices.
6. Inappropriate use of mobile devices is a serious offence: cases of misuse could lead to disciplinary action being taken against the individual concerned, as outlined within our company induction pack and disciplinary procedures.

*In the context of this policy "everyone" refers to Employees, freelance teachers, supply staff, students, volunteers, contractors and anyone else working for or on behalf of Ashbridge School Ltd.

Parents and visitors are not permitted to use any mobile device on site. Team members are expected to challenge any parents or visitors using their mobile phones on site in order to protect the children in our care. It is essential that all team members do this to ensure consistency and prevent confusion amongst customers and visitors.

Use of Tablets/iPads and school laptops/PCs

When using electronic devices as a tracking or teaching tool, or to share information with parents via Parent Zone or Seesaw, the following must be adhered to:-

- School and nursery Wi-Fi may be used but only teachers, teaching assistants, members of the Nursery Management Team (NMT) and Room Leaders may know the password.
- Apps can only be downloaded by the teacher/ member of the NMT, who must use their discretion when deciding whether the app is suitable or relevant.
- Any software which contains children's details, for example iConnect, must have a secure password to open it and tablets should be kept locked when not in use.
- All tablets must be secured in a safe place designated by the nursery manager at the end of the day and tablets must never be taken home.
- If laptops are taken home to facilitate home learning they must be kept in a secure location at home and any confidential information must be password protected.

Team members are permitted to use Twitter on the class iPads and must refer to the Twitter and photograph/video guidelines in this policy, together with the list of children who may not have photographs/videos taken.

USE OF CAMERAS AND PHOTOGRAPHS

Photographs and videos may only be taken by employees using company cameras or mobile devices. Company cameras, tablets and iPads must not be taken home and should not be accessible to parents, other non-staff members, or members of staff who are not in regulated activity. Images and videos are stored on company computers and any images and videos stored on tablets or devices must be transferred to computer or deleted within 12 months. Random checks on tablet devices will be carried out by Charlotte Bingham Brindle to ensure this takes place.

Teachers in school are likely to use live and recorded video as part of their live lessons when remote teaching and the procedures around this are set out in the Remote Learning Policy.

When taking photographs/videos of children for use on social media or in other publications, staff must follow these guidelines:

1. Only take photographs/videos of children whose parents or guardians have given consent.
2. Photographs/videos of children must not be taken in inappropriate areas of the school or nursery, eg nappy changing, toilets, changing for PE etc.
3. Photographs/videos should show children enjoying themselves and learning. Be aware of children without photo consent in large group shots.
4. Captions must not include the name of any child.
5. Photographs/videos of children appearing distressed or unhappy should not be used.

This is monitored by Grace Cole and Charlotte Bingham Brindle as required and any photographs not meeting the guidelines must not be used on social media or in any other publication.

If team members notice any suspicious use of cameras by other staff, parents/guardians, children or members of the public inside or outside the school or nursery premises it is their responsibility to report it to their Line Manager and/or

*In the context of this policy "everyone" refers to Employees, freelance teachers, supply staff, students, volunteers, contractors and anyone else working for or on behalf of Ashbridge School Ltd.

the DSL immediately. Suspicious use may include covert recording, people taking pictures from outside the grounds, parents taking photos of other children, staff using their own devices for photographs or videos etc.

CONFIDENTIALITY & DATA PROTECTION

It is the responsibility of everyone at Ashbridge to maintain confidentiality and protect data, including when using technology and working online. In addition to following the Confidentiality Policy, staff must adhere to the following:

1. Computers should be password protected, or in the event of this not being possible, confidential documents should be password protected.
2. Confidential data should not be stored on personal devices including laptops or pen drives unless it is encrypted or password protected.
3. Ensure confidential files stored within the 'Document Store' are password protected or have limited access to relevant people.
4. Confidential information should never be sent via personal email addresses.

In order to protect our computer system, a firewall is provided by the computer server and all routers also have firewall protection. All managers and teachers have individual email addresses that run through Microsoft Outlook. These email addresses for all school and nursery business and any remote access is password protected. These systems are managed and maintained by the ICT technician.

LINKS WITH PARENTS

At Ashbridge we place great emphasis on effective communication with parents and guardians and use the internet to our advantage when communicating with parents. School parents receive a weekly newsletter and all parents/guardians are encouraged to 'follow' us on Twitter and 'like' us on Facebook and Instagram. It is important that we help to educate parents/guardians about online safety and we do so by providing e-safety guides, links to relevant websites within the school and nursery welcome packs, and hosting Parent Workshops for both school and nursery parents. By equipping our parents and guardians with the knowledge they need to keep their children safe online we can provide a consistent message about the importance of online safety. Parents and guardians are able to access this policy via the company website.

REPORTING INAPPROPRIATE, HARMFUL AND/OR ILLEGAL CONTENT FOUND ACCIDENTALLY

If any team member comes across inappropriate or harmful content or find that children are able to access content or information that is deemed inappropriate or harmful, this must be reported to Charlotte Bingham Brindle immediately, detailing either the website address or the search term used to access the content. Steps will then be taken to ensure the content can no longer be accessed, using the filtering system.

In the case of illegal content such as; images of child sexual abuse including child pornography, content that advocates the doing of a terrorist act or content instructing or promoting crime or violence, Charlotte Bingham Brindle, Nazma Ahmed or Grace Cole must be contacted immediately. Illegal content will be reported to the police or other relevant body on the same day.

REPORTING STAFF BREACHES OF THE ONLINE SAFETY POLICY

It is everyone's responsibility to report any breaches of this policy or any deliberate illegal activity relating to technology. Examples of illegal offences include but are not limited to: accessing child sexual abuse images, pornography or information, accessing criminally obscene adult content and accessing content relating to the incitement of racial hatred or radicalisation. If any of these offences occur they must be reported to the DSL immediately, referring also to the Whistleblowing policy. Inappropriate use includes all the possible issues stated in

*In the context of this policy "everyone" refers to Employees, freelance teachers, supply staff, students, volunteers, contractors and anyone else working for or on behalf of Ashbridge School Ltd.

this policy, such as taking photographs/videos that don't follow the guidelines, storing confidential information on personal devices etc.

In the case of inappropriate internet use or breach of this policy, we expect all staff to follow procedures as set out in the Whistleblowing policy. If you are unsure if internet activity is illegal or inappropriate, it is always best to pass your concerns on to the relevant person.

As stated, breaches of this policy will be dealt with in line with the Disciplinary, Safeguarding and Child Protection Procedures.

*In the context of this policy "everyone" refers to Employees, freelance teachers, supply staff, students, volunteers, contractors and anyone else working for or on behalf of Ashbridge School Ltd.