Technology and Online Safety Policy

INTRODUCTION

This policy relates to all members of the school and nursery. It is updated annually or sooner if changes in technology, legislation requires it. It is monitored and approved by the Senior Management Team. This policy is promoted across the company and is available to parents and guardians on request and on the company website.

It is vital that our staff and children are sufficiently educated and know the policies and procedures to follow when working online or using modern technologies. 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 Policy, Anti-Bullying Strategy, Behaviour Policy and the Acceptable Use Policies: "Children in School", "Staff" and "Directors, Students, Freelance Teachers, Volunteers etc".

STAFF ROLES AND RESPONSIBILITIES

The school's Lead Person for Online Safety is Communication and Compliance Officer, Charlotte Bingham Brindle. It is their responsibility, together with the rest of the SMT 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, Steve Thorogood, to ensure the school's computer systems 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.

SAFEGUARDING CONCERNS

We provide an online environment that ensures children are protected from accessing harmful or inappropriate content without unreasonable blocking of websites, being subjected to harmful online interaction with others, or conducting themselves in a manner that increases the likelihood of, or causes, harm. The school's network has a filter system provided by OpenDNS and this is set to high settings in order to prevent children accessing inappropriate material. A children's search engine, Kiddle, and other safeguarding systems are also in place. Steve Thorougood manages this 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.

Regular staff training, staff vigilance and appropriate filtering systems mean we do all we reasonably can to limit children's exposure to online risks. Specific safeguarding issues relating to technology and online safety include, but are not exclusively:

- Cyberbullying
- Child sexual exploitation
- Gangs and youth violence
- Hate
- Radicalisation
- Terrorism and extremism
- Sexting (also known as youth-produced sexual imagery)

*In the context of this policy "everyone" refers to members of staff, students, Directors and anyone working in a voluntary or training capacity within the company.

SOCIAL MEDIA

Social media is an incredibly useful tool for communication and marketing and it is important that Ashbridge staff 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. Communication and Compliance Officer, 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.

Ashbridge Use of Social Media - Key Principles

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 the staff are not displayed in a negative way on any social media or messaging service, such as Whatsapp, Facebook, 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 social media or other messaging service, and should exercise caution when communicating with each other.** An exception to this would be when parents are already friends with staff outside of the work setting, although staff members should not discuss work matters with friends who are also parents of children at Ashbridge.

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 Headteacher/SMT. This applies to any published material on the internet or written documentation.
2. The posting by anyone of any communication or images which links employees, students or volunteers of the school and nursery to any form of illegal conduct or 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 on personal accounts of employees, children, parents, directors or anyone directly connected with the company whilst engaged in school/nursery activities.
5. Being 'friends' with customers on social networks, unless the friendship has formed outside the workplace.

Specific Guidelines Relating to Twitter

Twitter is a tool 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.

1. Staff must not use their personal Twitter accounts for school and nursery business. Each area should have an account in nursery and each class in school eg:- @ashbridgebabies or @ashbridgeyear6
2. Photos shared on Twitter must show children in a positive manner and follow the guidelines detailed in the "Use of Cameras and Photographs" section of this policy.
3. The names of children should not be included on any picture shared on Twitter.
4. Any photos or articles that are 're-tweeted' from individuals or companies must also follow the photo guidelines and be in line with the values of our company.

Potential and Actual Breaches of the Code of Conduct

Regular monitoring is carried out by Director of Operations, Grace Cole and Communications and Compliance Officer, 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.

*In the context of this policy "everyone" refers to members of staff, students, Directors and anyone working in a voluntary or training capacity within the company.

- 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 and Nursery 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.

Parental Use of 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.

If any parent is found to have posted 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 for a meeting and be asked to remove the comments 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.

USE OF MOBILE DEVICES

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

Personal Mobile Devices

1. Staff must not use personal mobile devices in any classroom or in any area designated for children. The only exception to this rule is when staff are in the forest or away on trips. Managers may also carry their phones in the case of Lockdown or fire evacuations.
2. Staff take their own mobile phones into the forest or on trips for communication with school and emergencies only. Staff are not permitted to use their own devices for personal use or taking photographs at any time when they are with children.
3. Staff 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. Staff are not permitted to use the schools Wi-Fi on their personal mobile devices without specific permission from the SMT.
5. Staff must not take or store photographs 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 procedures.

Mobile phone use on premises by customers and visitors

All customers and visitors are made aware that the use of mobile phones 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. Staff are expected to challenge any parents or visitors using their mobile phones on site.

Parents/guardians 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 Welcome Packs.

*In the context of this policy "everyone" refers to members of staff, students, Directors and anyone working in a voluntary or training capacity within the company.

Mobile device use on premises by pupils

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, portable games consoles and any other electronic device.

Use of Tablets/iPads

When using tablets as a tracking or teaching tool, the following must be adhered to:-

- School and nursery Wi-Fi may be used but only teachers, teaching assistants, Team Leaders and Room Leaders may know the password.
- Apps can only be downloaded by the teacher/ Team Leader, 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 iPads should be kept locked when not in use.

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

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
- 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 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 at any time.

Staff are also asked to give written permission for photographs and videos of them to be used when joining the company and we respect and adhere to each individual staff member's request.

Photographs may only be taken by staff 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 are stored on company computers and any images 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 Grace Cole and Charlotte Bingham Brindle to ensure this takes place.

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 by the SMT whilst 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.

Customers are not permitted to use any personal recording devices or personal cameras including cameras on mobile devices without prior consent from the Headteacher or member of the Senior Management Team. See also

*In the context of this policy "everyone" refers to members of staff, students, Directors and anyone working in a voluntary or training capacity within the company.

the company Mobile Device section of this policy. All members of staff are responsible for monitoring this and must politely ask parents, carers and visitors to refrain from using mobile phones on site.

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

1. Only take photographs of children whose parents or guardians have given consent.
2. Photographs of children must not be taken in inappropriate areas of the school or nursery, eg nappy changing, toilets, changing for PE etc.
3. Photographs should show children enjoying themselves and learning and should, where possible, include more than one child. Be aware of children without photo consent in large group shots.
4. Photograph captions must not include the name of any child.
5. Photographs 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 staff 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 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.

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, and hacking social network or email accounts.

Whilst we educate parents and children about the legal ages for social media platforms we recognise that some children do have accounts and we do all that is reasonably practical to discourage this and educate children and parents in the safe use of social media.

It is everyone's responsibility to monitor children's internet use whilst at school and report any incidents using the procedures set out in the Anti-Bullying and Safeguarding Policies. As detailed in this policy we use filtered internet access in school and nursery to protect our children from unsuitable content and teachers should report any issues with this to Charlotte Bingham Brindle.

It is essential that we build resilience by educating our children about internet safety, putting particular emphasis on how to deal with cyber-bullying and making them aware of age restrictions on social media platforms. Children learn about this as part of our Personal Development Programme, in Computing lessons and during events such as Safer Internet Day.

For more information on how Ashbridge deal with bullying and teach internet safety, please refer to the Anti-Bullying Policy and Computing Policy respectively.

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.
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. Each room in nursery at Lindle Lane and 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 ICT technician, Steve Thorogood.

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 by email and all parents/guardians are encouraged to 'follow' us on Twitter and 'like' us on Facebook. 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 member of staff 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, content that advocates the doing of a terrorist act or content instructing or promoting crime or violence, Charlotte Bingham Brindle 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 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 this policy, such as taking photographs 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 members of staff, students, Directors and anyone working in a voluntary or training capacity within the company.