TECHNOLOGY AND ONLINE SAFETY POLICY AND PROCEDURES

Approved by: SLT

Approved date: September 2024

To be reviewed by: SLT

Review date: September 2025

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, peripatetic 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, AI Policy, 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, as well as training on filtering and monitoring. The Lead Person for Online Safety is also responsible, together with support provider, Connectus Solutions and the IT 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. The proprietor holds overall responsibility for online safety and the Lead Person provides them with regular updates on online safety and any concerns.

CHILDREN

SAFEGUARDING CONCERNS

Keeping children safe online and providing them with the tools to stay safe online when out of school and nursery 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. Most of these areas refer to school as online safety teaching in nursery is much more based around early awareness and parent information. Children in nursery do not use technology with internet connectivity during the nursery day.

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 and/or misandry, 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. 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 or nursery 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 and throughout the school year.

Commerce

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 Connectus Solutions and it is everyone's responsibility to report any material that is harmful or inappropriate. Equally if someone is unable to access a website they require for teaching, learning, monitoring or assessment purposes, a support request should be raised. Reporting is managed by Connectus Solutions and the organisation's IT technician.

If children are required to undertake remote learning, safe, approved platforms including Microsoft Teams 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 and monitoring systems mean we do all we reasonably can to limit children's exposure to online risks.

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; hacking social network or email accounts; and the creation and/or distribution of fake material, including using AI technologies.

Though the PDP programme, Computing curriculum, Safer Internet Day and other teaching we encourage school 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 or nursery 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) in school children discuss the impacts of social media and gaming, both positive and negative.

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

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, smart glasses, portable games consoles and any other electronic device

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 setting directly and not through social media platforms. This includes direct messaging on the group's social media accounts or messaging members of staff individually. Organisation-owned social media accounts are only monitored during working hours.

If any parent or other family member of a child is found to have posted or shared anything about the organisation 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 as part of resolving 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 Parent Handbook

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 leadership 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 Handbooks.

It is an expectation of all team members that they politely challenge any member of the public, including children's family members, using a mobile phone or device on the school or nursery premises and direct them to a mobile phone zone. Team members are expected to immediately report to their line manager any failure to follow the mobile phone and device policy by other team members.

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/carers 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, and are available through iConnect. Parents/carers 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 organisation guidelines and are supervised whilst on the premises. A commercial company is also used to take individual and group photographs of children for purchase by parents/carers on approximately two occasions each year. These sessions and the procedures for management and distribution are supervised by the leadership team. Photographers are aware of their responsibilities and are required to act within our guidelines.

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

SOCIAL MEDIA

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 organisation as a whole. Early Years Quality Lead, Hannah Little, oversees all of our social media engagement.

Everyone* at Ashbridge has a responsibility to ensure that their use of social media platforms, both in and out of work, promotes the organisation in a positive way and upholds the Ashbridge reputation. It is important that the organisation or those who work for the organisation 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.

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 organisation'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 organisation. This includes defamatory comments.

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

3. The disclosure of confidential or business-sensitive information; or the disclosure of information or images that could compromise the security of the organisation.
4. The posting of any images/videos on personal accounts of employees, children, parents, directors or anyone directly connected with the organisation whilst engaged in school/nursery activities.
5. The posting of out-of-work activities whilst 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.

Potential and Actual Breaches of the Code of Conduct

Regular monitoring is carried out by members of the Senior Leadership Team. 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 organisation will take appropriate action in order to protect their reputation and that of its staff, parents and children and anyone else directly linked to Ashbridge School Ltd.

USE OF MOBILE DEVICES

The term 'mobile devices' refers to smart phones, tablets, smart watches, smart glasses 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. Managers and leaders may carry their phones in the case of Lockdown or fire evacuations to communicate with each other and the emergency services.
2. Employees are not permitted to wear any smartwatch with a watch style face. Basic fitness trackers may be worn but these must be removed when entering children's bathrooms or changing nappies.
2. Employees may take their own mobile phones on trips for communication with school and emergencies only, if an organisation-owed device is not available. 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 carers 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 the staff induction pack and disciplinary procedures.

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 organisation-owned devices such as tablets, laptops and 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.
- Any request for new apps or software must be directed to IT Support.
- Any software or website which contains children's details, for example iConnect and CPOMS, 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.
- Devices must never be left in cars overnight.

USE OF CAMERAS AND PHOTOGRAPHS

Photographs and videos may only be taken by employees using organisation-owned cameras or mobile devices. These cameras and tablets 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 organisation-owned devices and SharePoint and any images and videos stored on tablets or other devices must be transferred to computer or Sharepoint or deleted within 12 months.

If team members notice any suspicious use of cameras by other staff, parents/carers, children or members of the public in or around the school or nursery premises it is their responsibility to report it to their Line Manager and/or the DSL immediately, or challenge the person if they feel it is safe and appropriate to do so. 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 must 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. Confidential files stored within SharePoint should 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 in place. All staff have individual email addresses that run through Microsoft Outlook, although email accounts for Nursery Practitioners and Room Leaders are restricted to receive incoming email only. These email addresses are only to be used for school and nursery business. These systems are managed and maintained by Connectus Solutions and the company's ICT technician.

LINKS WITH PARENTS

We place great emphasis on effective communication with parents and carers. Parents are encouraged to follow and engage with us on social media and are sent regular updates and communications via email and ParentZone. It is important that we help to educate parents/carers about online safety and we do so by providing e-safety guides and sharing other relevant information. By equipping our parents and carers 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 carers are able to access this policy via the organisation's 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 the Director of Compliance and IT Support 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 undertaking a terrorist act or content instructing or promoting crime or violence a Designated Safeguarding Lead 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. Examples of illegal offences include but are not limited to: accessing child sexual abuse images, child pornography, criminally obscene adult content and 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/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.