Name:	Hart Hill Nursery School
Type:	LA (Maintained) Nursery School
Local Authority:	Luton
Registered:	08/11/2022
Last Update:	08/11/2022
Last Login:	16/06/2023
Aspects Complete:	11 / 11
Level:	2.6
Progress:	50%

Technology

KT Devices

Level: 3 | National: 3.4 | Progress: 50%

Your Level: Level 3 (Essentials)

The online safety policy includes guidance for all users and visitors on the safe use of devices within the setting and these are included in clear and acknowledged acceptable use agreements Rules on mobile device use are clearly signposted for visitors All users are able to identify and feel confident in challenging misuse All users know how to report issues to the online safety lead

Recommendations for Improvement

Technology and associated behaviours and risks change rapidly. Allow time to review your current strategy and ensure any new risks are addressed in policy and practice.

Audit the devices that your setting provides and ensure their professional use is regulated and managed. This might include computers; laptops; cameras; tablets and official mobile phones.

It's important to also understand staff/volunteer use of personal devices whilst in your setting. A voluntary audit of personal devices will assist in developing a clear set of expectations on their use e.g. personal calls at breaktime; device free areas; storage in lockers etc.

Staff/volunteers should not be using personal devices for their professional role within your setting e.g. contacting parents/families; taking images/video; personal details of setting users etc.

KT Security

Level: 3 | National: 3.3 | Progress: 50%

Your Level: Level 3 (Essentials)

Setting devices are appropriately protected against physical and technical security threats Staff/volunteer use of devices is managed through appropriate password access Staff/volunteer have been briefed on the importance of technical security and practice secure behaviour when using setting devices Where the internet is used, access is managed and children are supervised and use child-friendly search engines Where the internet is used, access to illegal content is blocked through effective filtering

Recommendations for Improvement

Review the devices in your setting and setup automatic updates for operating system security patches and latest anti-virus / malware lists to ensure they are protected from emerging threats.

For settings with a larger number of devices or network equipment, develop ways to improve technical expertise, either from amongst your own staff/volunteers or through an external support service.

Further develop your own staff/volunteers' expertise through regular updates and awareness raising, particularly as new threats emerge.

Where the internet is used, ensure appropriate filtering is in place to prevent access to inappropriate online content. You should also understand how and where your internet is being used through appropriate monitoring. This could range from physical supervision to more technical solutions and the results of this should be regularly reviewed.

Regularly review your technical security strategy as threats, behaviours and technology changes.

KT Digital Images

Level: 3 National: 3.6 Progress: 50%

Your Level: Level 3 (Essentials)

The setting provides devices for staff/volunteers to take digital images or record video for professional use Staff/volunteers are aware of the potential safeguarding risks in the use of digital image/video. Permissions have been gained from parents/carers for taking and use of digital image/video of children. Staff/volunteers are aware of children whose images may not be taken or used. There is clear guidance on the sharing and publication of children's images and mechanisms are in place for the secure sharing of images e.g. through secure parental sites; secure emails etc. Any use of CCTV/premises video recording meets statutory and safeguarding requirements, that they are technically secured and that its use is referenced in setting policies. The setting stores images securely and meets legal requirements on how long they may be kept.

Recommendations for Improvement

Regularly review how permissions are gained, used and kept up to date e.g new admissions; children leaving. Use these permissions to regularly brief staff/volunteers on children whose images must not be taken or shared.

Ensure that parents/carers are clear about your guidance on the taking and publication of children's images. Parents/carers should not be prevented from taking images of their children at events but need to be aware that they should not publish or share beyond the use of their own family group. NSPCC guidance on sharing of children's images.

Review your policy and practice in the light of changes to national guidance and emerging threats.

KT Social Media & Communication

Level: 3 National: 3.5 Progress: 50%

Your Level: Level 3 (Essentials)

All communications take place through clear and established setting systems and are professional in nature Where social media is used to communicate with the setting community, it is responsibly managed and content is checked Where websites are used to publish information, they are responsibly managed and content checked. Communications are monitored for concerns/complaints Staff/volunteers are aware of how their personal use of social media may affect their role

▸ Recommendations for Improvement

Ensure that there is a clear communication strategy which staff/volunteers understand and follow. SWGfL provide school policy templates for Social Media and Communications that may be useful in building the key areas of an early years strategy. Provide advice and guidance for the safe and responsible use of all your communication technologies.

Any public facing communications should only be used if officially agreed by the setting and should be regularly monitored for appropriate content and use. This could be through an appointed person responsible for ensuring communications are professional and appropriate or monitoring technologies e.g. SWGfL Reputation Alerts

Communication technologies also offer a gateway for the wider community to register concerns or complaints. It is important for any setting to identify these quickly and respond to them in an appropriate way, particularly if they involve child safety, staff/volunteer abuse or reputational damage. Ensure your complaints procedure takes this into account. SWGfL Whisper is a reporting tool that provides an anonymous route to safely share concerns.

Ensure that all staff and volunteers understand the risks associated with the use of these communication technologies and are encouraged to be responsible users.

Management

KT Responsibilities

Level: 2 National: 3.1 Progress: 50%

▸ Your Level: Level 2 (Planning)

Plans are in place to appoint an online safety lead but these still require defining or co-ordinating.

▸ Recommendations for Improvement

Appoint a suitable person to lead online safety. Ensure they are clear about their role and are supported in this. They may need time to get up to speed with areas like policy and developing their own expertise and understanding. Encourage other staff to be involved in developing your new online safeguarding strategy. This improves ownership and relevance.

KT Policy

Level: 3 | National: 3.3 | Progress: 50%

Your Level: Level 3 (Essentials)

Policies and guidance are in place for informing the online safety of all users in your setting. Your online safety policy meets statutory requirements. (See "Safeguarding Focus") There is an acceptable use agreement in place for all staff/volunteers and visitors which is clearly communicated.

Recommendations for Improvement

Promote your online safety policy to all staff/volunteers so that expectations are clear and understood. Make sure your acceptable use agreement for visitors/adults is clearly communicated when they enter your setting.

Develop a simple set of acceptable use rules for children that they can understand.

Review your policy sets regularly in the light of changes in legislation, practice and developments in technology.

Ensure your online safety policy is integrated into and consistent with other relevant policies, in particular the child protection and safeguarding policies.

KT Safeguarding

Level: 2 National: 3.3 Progress: 50%

Your Level: Level 2 (Planning)

There are some references to online safety in existing safeguarding policy and practice but these are neither consistent nor cover statutory requirements.

Recommendations for Improvement

Review existing safeguarding policies and add online safety obligations, as required. Check that all references to online safety are consistent across all policy sets.

Develop protocols for the reporting of online safety incidents, within existing safeguarding routes.

Through briefings, ensure that staff/volunteers are aware of these online safety elements in the safeguarding and related policies and that they know and understand how to respond to online safety incidents/reports.

Ensure that there are processes in place to deal with online safety incidents that affect staff/volunteers, to both review incidents and protect staff/volunteers.

Develop processes to review incidents and how the outcomes lead to improvements in policy and practice.

People

KT Personal Data

Level: 3 National: 3.5 Progress: 50%

Your Level: Level 3 (Essentials)

The setting has paid the data protection fee with the ICO There is a clear data protection policy in place Special category personal data is protected Lawful basis for holding personal data is clear and consent has been gained for any additional personal data use There is a clear privacy notice that has been shared

with all users Staff/volunteers are aware of their responsibilities when managing personal data as part of their role

▸ Recommendations for Improvement

As people arrive and leave your setting, you may end up storing personal data that is no longer actively being used. You may be required to keep some data for a specific time period. Advice and guidance on record keeping can be found on this PACEY factsheet.

For each new initiative you introduce, consider the level of risk to personal data used and how it relates to your policy and duty of care. This is sometimes referred to as a Data Protection Impact Assessment (DPIA) but involves the setting making sure that the sharing of information about those involved remains legal and secure.

If you suspect the personal data you hold is breached or compromised, you must report it to the ICO within 72 hours. However, this does not need to happen every time there is a breach, only when there is risk to people. You can carry out a self-assessment to work out if you should make a report. Be sure to train your staff about your expectations should a breach occur.

Every user has the right to ask an organisation what information they hold about them. This is called a Subject Access Request (SAR). There are rules about whether you should respond, how and how quickly. This guide from the ICO may help. You may wish to have a policy for SARs in place to share with users.

As with many other administration procedures, there is a legal duty to keep clear records of incidents or requests with which you have dealt. This should be managed by the DPO and reviewed frequently. This helps inform practice, identify trends and weaknesses in procedure. Guidance is available from the ICO.

KT Responding to Issues

Level: 2 National: 3.2 Progress: 50%

Your Level: Level 2 (Planning)

The setting has identified the need to improve safeguarding practice and is developing its effectiveness in responding to online safety issues.

Recommendations for Improvement

Effective reporting relies on a consistent response each time an issue is shared. Not only does this ensure that online safety issues are dealt with in the same way as any other safeguarding issue, but it also builds confidence in the process from users. If they know reporting will help them resolve issues, they are more likely to seek help.

All staff need to be able to recognise an issue when it arises and should be confident and consistent in their response. Bring all staff on board and empower them through regular online safety briefings and updates.

Your online safety lead should be the first port of call for reporting online safety issues so make people aware of who they should go to for guidance and support.

Your response to online safety incidents should be informed by your existing safeguarding procedures and reporting routes. Where there is significant potential for harm, they should have the same priority as physical safeguarding.

Explore other ways for people to bring issues to your attention: a confidential email address; anonymous reporting routes on your website (eg SWGfL Whisper) or messaging app.

Establish procedures for immediately reporting serious incidents to the relevant agencies e.g. police; health; social care etc

Think about how you might record incidents. A simple log book or a spreadsheet would be a good start.

KT Educating Children

Level: 3 National: 2.8 Progress: 50%

Your Level: Level 3 (Essentials)

There is clear evidence that online safety is being discussed with children. There is provision to follow up online safety issues with relevant discussions that guide children and reduce potential harm. Where appropriate, the setting is building links with outside expert advice eg police; charities and other agencies to support its programme.

Recommendations for Improvement

Ensure your staff/volunteer safeguarding training includes online safety and that this informs and is embedded within your education programme. Review your current programme and identify where online safety could be interwoven (eg when thinking about communicating; making friends; playing; getting help etc). Find opportunities for adults to model safe practice when using technology with children. Evidence these opportunities within your planning. Build activities around Safer Internet Day each year to celebrate your achievements; involve families and local agencies in those events to inform your programme and increase awareness. Find ways that allow children to share their thoughts and experiences that could contribute to the wider online safety culture.

KT Training Adults

Level: 2 National: 2.9 Progress: 50%

Your Level: Level 2 (Planning)

Online safety training is available for some staff and volunteers but is neither consistent, nor planned.

Recommendations for Improvement

Begin to plan online safety into your annual safeguarding training for all staff and volunteers. Work to ensure that online safety training is consistent with your existing safeguarding culture.