



# The Federation of Duke Street and Highfield Nursery Schools

## **Online Safety Policy (Including the Acceptable Use Policy) Revised and Updated September 2025**

|  |  |
|--|--|
| Policy Leader / DSL / EHT*   | <b>Susan Conron, Executive Headteacher and DSL</b> |
| Last Updated by School   | <b>09/09/25</b>                                    |
| Governor with lead responsibility for online safety & cyber safety | <i>Karen Stephens</i>                              |
| CP & Safeguarding governor:  | Hellen Hull  |
| Communicated to staff via email                                    | Annual updates 30/09/25                            |

**Our online safety vision statement;**  
**"To equip children in a technology driven world with the skills and knowledge they need to use technology safely; safeguarding their wellbeing to instil healthy habits and attitudes towards technology at the school, in the home and beyond."**

## **Online Policy**

Technology plays a significant role in our lives and influences on young children cannot be overlooked.

By introducing digital technology in a controlled and supervised way we can help children develop essential skills to: understand and navigate online platforms; practice responsible online behaviour and protecting personal information.

Through safe technology we can empower children to make informed choices and develop critical thinking skills without stifling or limiting their curiosity but equipping them with knowledge, skills and attitudes to thrive in a digital society whilst safeguarding their wellbeing. Online encompasses Internet technologies and electronic communications such as mobile phones as well as collaboration tools and personal publishing such as online 'blogs' and online forums including Twitter and Facebook. It highlights the need to educate staff and children about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

The school's Online Safety policy operates in conjunction with other policies including those for Child Protection, Positive Behaviour (including Care and Control of pupils; Bullying), Safeguarding, Data Protection and Security.

The policy has been discussed and approved by the children, parents, staff and governors and is based on the recent recommendations within Kcsie 2025; Education Digital Services LCC; Online Safety Governance checklist; NOS, National College updates. The purpose of these measures is to protect users, the school and LCC and to make the use of online technologies a safer and more enjoyable experience.

The Online Safety Policy identifies and provides guidance on the following: importance of online safety; online risks in early years settings; online risks at home; strategies to minimise risks; personal online safety and processes of how to report any concerns relating to any member of the school digital community and their use of the school digital identity.

## Good Practice Regarding Online Safety

Online Safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and children; encouraged by education and made explicit through published policies.
- Sound implementation of Online Safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure Giga fast Broadband. DSL/HT and SBM have effective management of Net sweeper online filtering and Net sweeper on guard; for real time information.
- CLEO Secure Schools Network and Sophos Central (Anti-Virus and Threat Protection Service) which provides school with licences for a comprehensive suite of technologies to protect all school devices from a wide variety of threats.
- National Education Network standards and specifications.

### Further Information

For details of Online Safety in Lancashire schools;

For cyber-bullying or digital safety concerns;

The Safer Internet Centre 0844 381 4772

<https://saferinternet.org.uk/>

The following documents have been used for reference:

<http://www.lancshiresafeguarding.org.uk/online-safeguarding/schools-the-childrens-workforce.aspx>

<http://www.lancshiresafeguarding.org.uk/online-safeguarding/news-events.aspx>

<https://www.nspcc.org.uk/keeping-children-safe/online-safety/>

National online safety updates via The National College.

InternetMatters.org

## Introduction

### Writing and reviewing the Online Safety policy

The Online Safety Policy is part of the School Development Plan and relates to other policies including those for all curricular subjects, behaviour (including care & control of pupils and bullying), cyber security and child protection.

- Federation of Duke Street & Highfield Nursery Schools Online Safety co-ordinators Mrs Susan Conron ( Head Teacher) supported by Mrs Lynne Dickinson (DS) and Claire Bland (Hf)

- Our Online Safety Policy has been written by the school, building on the Lancashire Online Safeguarding Strategy and government guidance and online safety updates from Kcsie and The National College. It has been agreed by senior management and approved by governors
- The Online Safety Policy and its implementation will be reviewed annually.
- The governor with lead responsibility for cyber safety is Karen Stephens
- The online safety governance audit will be completed by a named Governor on:

In our obligation to "Keeping Children Safe in Education" The self review tools are:

**360degree safe**, an online safety self review tool for schools. Every year, the data collected through the tool is analysed to see the common trends. <https://360safe.org.uk/>

**Project Evolve**, is a free toolkit that covers all aspects of the UKCIS "Education in a connected world" Framework, across all age phases from nursery to 18 years. <https://projectevolve.co.uk>

[Dfe self assessment tool](#) for filtering and monitoring

## The School's Online Safety Co-ordinator

The Online Safety Co-ordinator /DSL is the main point of contact for Online Safety related issues and incidents. The role of the Online Safety Co-ordinator/DSL includes but is not limited to:

- Having operational responsibility for ensuring the development, maintenance and review of the school's Online Safety Policy and associated documents, including Acceptable Use Policies.
- Ensuring that the policy is implemented and that compliance with the policy is actively monitored.
- Provide means which practitioners can be equipped with knowledge and skills to demonstrate schools commitment to online safety.
- Ensuring all staff are aware of procedures how to report a concern from the school digital community or acceptable use concern.
- Liaison with school admin support to ensure Netsweeper filtering reports are received and suspicious search reports investigated and action taken if required. Weekly reports are generated and emailed to bursar and head each week. These are checked; reviewed and retained to evidence our robust procedures.
- Recent addition of Netsweeper Onguard, to provide cloud-based monitoring software to identify and categorise potential safeguarding incidents. The software record details of these for review by school's safeguarding lead.
- All school equipment to have correct control settings to block and restrict age appropriate material.
- Keeping personally up-to-date with Online Safety issues and guidance through liaison with NOS; NSPCC digital online safety; the Local

Authority and through advice given by national agencies such as the Child Exploitation and Online Protection Centre (CEOP).

- Parents and carers provide a vital role in promoting balanced approach to online activity; we can provide further information and support if parents do not have the knowledge/tools to promote safe online behaviour.
- Providing or arranging Online Safety advice/training for staff, parents/carers and governors. All staff and governors have access to National College CPD platform which has a wide variety of resource/advice to assist with the obligation of Keeping Children Safe in Education.
- Lead by example a culture to develop a positive attitude towards devices to ensure all staff/governors/parents promote the use of digital devices in a respectful way; modelling appropriate adult behaviours within setting
- Ensuring the Head, SLT, staff, children and governors are updated as necessary; parents are provided on a termly basis with an online safety guidance document; including useful links. Parents and governors are also provided bi-annually with the free [Vodafone Digital Parenting](#) on all current matters relating to internet safety. [UK internet safety](#)
- A coordinated approach across relevant safeguarding areas.
- Ensure updated guidance is observed and included in adaption of policies to demonstrate compliance.
- DSL's also liaise with curriculum leads and technical services to ensure all aspects of online safety is

Some of the above responsibilities may be delegated to appropriate members of staff.

# Security and Data Management

The Lancashire Safeguarding Children's Board have recognised in their Online Safeguarding Strategy that the four strategic objectives below provide a framework structure within schools can address the variety of Online Safety aspects in a structured and meaningful way.

These strategic objectives are:

1. **Safer Management:** To ensure your school/college/establishment has robust and effective policies, practices and procedures to safeguard Children and Young People (C&YP) against online safety risks.
2. **Safer Access:** To identify and promote technologies, tools and infrastructure services which appropriately support Online Safeguarding priorities for the School, C&YP and related stakeholders. The following details will assist you in meeting this Strategic Objective:
  - Connectivity (Broadband) – Lancashire County Council Education Digital Services provides the CLEO Secure Schools Network with a private Wide-Area Network (WAN), see paragraph below
  - System policies (passwords; e-mail ;) - Further information on passwords including the "perfect passwords checklist" can be found at <https://www.saferinternet.org.uk/blog/manage-your-safety-and-security-online>
  - Web Filtering & Monitoring Systems – Lancashire County Council Education Digital Services provides secure web filtering using Netsweeper Systems
  - Technical Security (Anti-virus & malware protection, backups & recovery, network resilience, physical security, network security, remote access) – Lancashire County Council Education Digital Services offers SOPHOS anti-virus protection, RBUSS data backup, a dedicated security team and a technical helpdesk,
  - Web Filtering Reporting – Reporting is available using Netsweeper Web Filtering please see the [web filtering guide](#)
3. **Safer Learning:** Consider learning opportunities for all stakeholders (e.g. Pupils/Students, Staff, Governors, Parents/Carers and the wider Community) to raise awareness of potential risks and how to report and manage them.
4. **Safer Standards:** Consider how Online Safety is audited and reviewed within your setting.

Microsoft Teams is used as a shared platform to access and share document.

All staff have unique identities and use MFA

ICT security is a complex subject that involves all technology users in the school, dealing with issues regarding the collection and storage of data through to the physical security of equipment.

Connectivity (Broadband) – Lancashire County Council Education Digital Services provides the CLEO Secure Schools Network with a private Wide-Area Network (WAN), see paragraph below

Under the Data Protection Act 2018 all sensitive or personal data is recorded, processed, transferred and made available for access in school. This data must be:

- Accurate
- Secure
- Fairly and lawfully processed
- Processed for limited purposes
- Processed in accordance with the data subject's rights
- Adequate, relevant and not excessive
- Kept no longer than is necessary
- Only transferred to others with adequate protection.

All data in school must be kept secure and staff informed of what they can or can't do with data through the Online Safety Policy; Code of Conduct; Social Media policy; and Acceptable use statements.

**Acceptable use:** All staff are informed that they are able to use the school's wifi on personal devices for personal use during allocated lunchbreak.

Staff are also reminded that any site searches using the school wifi will be pulled on the weekly netsweeper report to be analysed and reviewed by the HT and SBM.

In the event of a suspicious search result; procedures will be followed to investigate the result to establish if any areas of concern are highlighted.

Depending on your role in school you will have access to different network drives.

The head teacher has access to all areas.

**Supply teachers** do not have access to the school drives and are unable to save onto computers.

RBUSS storage is carried out and supported. Our "Full System Backup" ensures improved disaster recovery options, reflecting advice from NCSC to ensure all important data is backed up. Data on the curricular and admin system is backed up RBUSS remote back up which is part of the service level agreement with Education Digital services. EDS

monitors back-up of data and deletes older back-ups when they are no longer required, all data is encrypted.

**For security issues; staff are NOT permitted** to use pen drives and other similar devices to transfer personal information such as reports, tracking, children's names and pictures.

**Staff are reminded to regularly change passwords to** maximise security of data and as set out in the code of conduct they have a responsibility to keep all technology safe and secure and looked after.

Assessment data, such as 'Trackers', are stored on the (HF 'Teaching and learning' drive on the school network, access to which is restricted by password to SMT staff only).

(DS office drive on the school network, access to which is restricted by password to SLT and office staff only). Staff are instructed not to store electronic copies of this data at home.

All user accounts are password protected and staff must change their password every 60 days for added security.

The following members of staff have remote Global desktop access, Lynne Dickinson, Gemma Devlin; specifically, to access Sims.net during periods of school closure/school holidays.

ICT Education Digital services half termly visits check a variety of issues including; Data Backup; Server Manager; Disc Capacity; UPS Status; Net sweeper filter checks; any other alerts.

Net sweeper filter checks are set to run every Sunday and the Bursar and Headteacher email addresses receive the following reports:

- 1) Suspicious search history over the previous 7 days.

The result of this report flags up anything of a concern to be further risk assessed and investigated further.

- 2) Net sweeper On guard provides cloud-based monitoring software to identify and categorise potential safeguarding incidents. The software record details of these for review by school safeguarding lead.

In addition: - admin in both schools carry out filtering tests and record and share the findings with HT and ICT co-ordinator <https://swgfl.org.uk/services/test-filtering/>

School does allow the use of 'cloud' storage facilities e.g. Dropbox / SkyDrive / Google docs and Moodle for external storage that is non confidential data.



At Duke Street & Highfield Nursery School Federation we have one wireless network in each school which is secure.

## The Use of Mobile Devices

School use of mobile devices, including laptops, tablets, mobile phones and cameras are commonplace in a technology driven world. Whilst these can provide a flexible solution and offer a range of exciting opportunities to extend children's learning, their use poses challenges in terms of online safety. Many of these devices integrate functionality to take images, access the Internet and engage users in various methods of external communication.

### Mobile phones

Mobile phones can present a variety of challenges if not used appropriately. Smart phones can upload pictures onto cloud storage so even if you delete picture from phones memory, it's still stored on cloud. They are valuable items that can be lost, stolen or damaged in the school environment and could also be considered as distracting or intrusive in a teaching or learning situation. However, staff and parents may equally have valid reasons why mobile phones should be readily available.

In order to balance the benefits of mobile phones alongside the possible issues they can create, the school has several guidelines in place:

- Staff are permitted to use mobile phones in school before the start of the school day at lunch and after the school day has ended; as previously stated; **in line with acceptable use** staff are informed that any searches on their phones during this time using school Wi-Fi is reported on via the weekly net sweeper results and all elements of **acceptable use** are to be observed.
- Children are not permitted to have mobile phones in school
- Parents are asked not to use mobile phones inside the school premises or outside when children are playing. Reminder signs are on entrances into children's environment.
- Staff are responsible for the security of their own belongings, including mobile phones, and, on request, can store them securely in the school office.
- Staff are advised to leave mobile phones in a locker or a safe place out of the children's environment. School provides lockers for personal items in school.
- **Images of children video or audio must not be recorded on personal mobile phones.**

### Reference Federation Safeguarding Policy 2025 Online Safety.

- The school office can always be contacted in the event of an emergency.

- **Warning!** Mobile phones have access to the Internet; this is NOT filtered and could lead to unsuitable content being viewed.
- Any suspicious use of mobile phones and / or cameras, report to a Susan Conron, Lynne Dickinson.

## **Other mobile devices**

The rules for mobile phone use in school apply to all other mobile devices.

- When permission to use such devices is granted it is expected that the relevant security settings, such as passwords and anti-viral protection, are in place and up to date.
- The owners of the devices are responsible for ensuring that all the content held on them is legal and should understand that the school cannot be held liable e.g. for any damage or theft of personal devices.
- Such devices can only be used on the school's network, e.g. to transfer data by Blue-Tooth or to access the Internet using Wi-Fi, after obtaining the express permission of the head teacher and should be checked first to ensure that they contain no viruses or mal-ware that may cause damage to the school's systems.
- As with mobile phones, inappropriate use of such devices may lead to their confiscation.
- Visitors (visiting professionals/students) to the setting who wish to use school wifi to be reminded of the online safety policy and the Netsweeper weekly reports which track internet searches over every 7 day period.
- Iwatches are permitted as long as they don't take photos. If a watch has the facility to answer/make a phone call the settings need to be adjusted so that this is not active during the school day.

## **Use of digital media (ipads and recording devices)**

The use of ipads and sound recording devices offer substantial benefits to education but equally present schools with challenges particularly regarding publishing or sharing media on the Internet, e.g. on Social Network sites. Photographs and videos of children and adults may be considered as personal data in terms of The Data Protection Act (2018).

## **Consent and Purpose**

- Written consent is collected from parents for photographs of their children to be taken or used. Permissions form is completed by parents for each child at the time of induction into Nursery
- Staff are informed of any children whose parents or guardians have not given their consent for their photographs to be taken or their images used in digital form by the school. Location = Children/year/important information. A list is compiled by the school office and is updated

when consent forms are reissued. It is the responsibility of staff to ensure that only images containing children whose parents or guardians have given permission are used by the school. Verbal consent is not considered acceptable.

- Images of staff or adults employed in the school will not be used without their permission (written). Full details for staff is available in the Code of Conduct document.
- It is made very clear, when gaining consent, how photographs can / cannot be used (including the use of external photographers or involvement of 3rd parties).
- Written consent includes permission to store / use images once a child has left the school e.g. for brochures, displays etc... Parents should be informed of the timescale for which images will be retained.
- Online permission forms are issued to parents prior to child starting Nursery. In the event of any circumstances that may necessitate removal of permission the list of children will be amended and reissued to all staff concerned.
- Parents are informed of the purposes for which images may be taken and used e.g. displays, website, brochures, press and other external media.
- Images that at times may be displayed in public areas, e.g. the entrance hall, are subject to the same restrictions.
- **Parental permission is required** for their child's images to be included in portfolios maintained by trainees and students not directly employed by the school.
- Parental permission is required to use group images in individual children's profiles. Where possible individual children's profiles are used for their own documents; and obscuring of other children's faces to prevent identification.
- Images are not used of children or adults who have left the school unless their written permission has been obtained.
- Written permission from parents (via an online permission form) is required when children's images are used by the press. Permission is required if the press wish to name individual children to accompany a photograph or if the media publish an image in their online publication which may offer facilities for the 'public' to add comments in relation to a story or image and can potentially invite negative as well as positive comments.

## **Taking Photographs / Video**

- Teachers and Early Years Practitioners authorised to take images related to the curriculum. Other adults taking photographs must be designated by the head teacher.
- Photographs and videos are only taken using **school owned tablets**. The use of personal equipment to store images must be avoided.
- When taking photographs and video the rights of an individual to refuse to be photographed are respected.

- Photographs must never show children who are distressed, injured or in a context that could be embarrassing or misinterpreted.
- Care is taken to ensure that individual children are not continually favoured when taking images.
- The subject of any film or photograph must be appropriately dressed and not participating in activities that could be misinterpreted e.g, particular care may be needed with the angle of shots for children engaged in PE activities.
- Certain locations are considered 'off limits' for taking photographs, e.g. toilets, cubicles, etc...
- Discretion must be applied with the use of close up shots as these may be considered intrusive. Shots should preferably include a background context and show children in group situations.

## Parents Taking Photographs / Videos

Under the Data Protection Act (2018), parents are entitled to take photographs of **their own** children on the provision that the images are for **their own** use, e.g. at a school production. Including other children or other purpose could constitute a potential breach of Data Protection legislation.

- Parents are informed that they should only take photographs of their own children and that they need permission to include any other children / adults.
- As it is virtually impossible for school to monitor parental pictures the school now publishes pictures on the school website after pictures are checked for permissions. Any other images wished to be used prior parental consent is required and must be obtained by the keyworker/school staff.
- Parents are reminded, in writing, that publishing images which include children other than their own or other adults on Social Network sites is not acceptable, unless specific permission has been obtained from the subjects and, in the case of children, their parents.

## Storage of Photographs / Video

- Staff are reminded that good housekeeping is vital to clear off old photos once children are no longer on roll. This should be done annually; unless a sooner frequency is required.
- It is keyworker responsibility to ***delete old photos from their devices once a child has left their group/school.***
- Photographs are securely stored and should not be removed from the school environment unless for a specific purpose and with the head teacher's consent. In this instance the data must be kept secure and must be erased after use. This could include storage of images on portable devices e.g. laptops or tablets.

- Images should be stored on tablets for the minimal amount of time. Only images intended for a specific purpose should be stored. They must be stored securely and be deleted once they have been used
- Cloud storage is used for Ipads but checked and deleted regularly.
- Staff should not store images on personal equipment e.g. tablets, laptops; as laid out in code of conduct and acceptable use.
- Staff should not store personal images on school equipment unless they have a clear purpose e.g. to support in the teaching of a lesson. Once used, the images should be deleted.
- Access to photographs / videos stored on school's equipment is restricted to school staff. The server allows data to be stored so that it is accessible either to all staff, teachers or pupils.
- Individual members of staff are responsible for deleting photographs / video or disposing of printed copies (e.g. by shredding) once the purpose for the image has lapsed. The ICT Technician has access to all areas of the network and can assist with the removal of data.
- Should a parent withdraw permission **the key worker is responsible** for the removal and deletion of images and may be assisted by the ICT Technician.
- Photographs sent electronically must be sent securely. This is done using staff accounts on the Lancashire e-mail system.

## **Publication of Photographs / Videos**

- Consent is needed from parents for publication of children's images, e.g. on a website and is completed at time of induction via the online form/permission.
- Photographs should only be published online to secure sites.
- When publishing photographs, care should be taken over the choice of images to ensure that individual children / adults cannot be identified or their image made available for downloading or misuse, e.g. through the use of low definition images that will not magnify effectively, e.g. using Image Resizer in Windows or the flash upload app on the school website.
- Full names and / or other personal information should not accompany published images.

- The Federation uses a secure online learning journal “Tapestry”



We are very proud of the trust placed in us by so many schools, settings, childminders, and families to take care of the data added to Tapestry. We take our responsibility to look after it very seriously.

This takes form in a number of ways, including being careful about who we employ, ensuring all of the software we use is up to date and fully tested, encrypting your data on our servers and the connections between you and our servers, and hiring independent companies to check our systems are secure (this is known as penetration testing).

We also back up your data in a completely separate location. This means that in the unlikely event that your data is lost or corrupted on the main servers, we can restore your data from those.

We don't sell the data added to Tapestry, use it for advertising, or make it visible to anyone who hasn't been authorised by the school, setting, or childminder who owns the account.

Despite all of that, security is only as strong as the weakest link. We therefore need to work with you, the people accessing and adding to the account, to ensure the overall system is secure. This means, for example, making sure you set safe passwords that you do not share with others, and that you know exactly who you are giving access to.

We agree and pay for a Tapestry subscription and agreement which is signed annually.

Tapestry is an online journal platform which is passworded and secure communication/share tool between keyworkers and parents.

## **When publishing images**

- School has a Facebook site; all permissions relating to their child's image being used on the Facebook site are obtained prior to the child starting by way of the online form/permissions.
- No images should be attached to personal social network sites.
- Personal social network sites; staff should ensure that personal profiles are secured and do not display content detrimental to their own professional status – as covered in the code of conduct and social media policy [Social Networking & Social Media](#) ; staff should recognise and understand the risks associated with publishing images.
- Staff and children are made aware that full names and personal details will not be used on any digital media, particularly in association with photographs

## **The Media, 3rd Parties and Copyright**

- Visiting third parties within school are supervised at all times whilst in the school and are expected to comply with the Data Protection requirements in terms of taking, storage and transfer of images.
- The copyright for images taken by a 3rd party must be made clear beforehand and agreed by the school and parents before such images are used, e.g. in a local newspaper.
- If uploading images to a 3rd party website, e.g. for printing or creating calendars, cards etc, staff are expected to read and be familiar with the terms and conditions of the web site. (You could unknowingly be granting the site's host licence to modify copy or redistribute your images without further consent. The site may also be advertised for 'personal use' only – therefore using for business purposes would be a breach of the terms and conditions).

## **Communication technologies**

School uses a variety of communication technologies, each of which carries various benefits and associated risks. All new technologies should be risk assessed against the potential benefits to learning and teaching before being employed throughout the school. Ideally this should be done before multiple devices are purchased. As new technologies are introduced, the Online Safety Policy will be updated and all users made aware of the changes. The policy is reviewed annually.

### **Email**

- The Lancashire Office 365 service is the preferred school email system.
- Extra measure of multi factor authentication is now used by all school federation staff; as an extra measure when accessing their online school email accounts on different devices.
- Staff should not access personal email accounts during school hours on school equipment unless prior permission is obtained from the head teacher and access is required for professional purposes.
- Only official email addresses should be used to contact staff.
- Office 365 Learning filtering service is employed to reduce the amount of SPAM (Junk Mail) received on school email accounts.
- All users should be aware of the risks of accessing content including SPAM, phishing, unsuitable materials and viruses from external email accounts, e.g. Hotmail or Gmail. Notices put in staffroom of new SPAM outbreaks.
- All users should be aware that email is covered by The Data Protection Act (2018) and the Freedom of Information Act (2000), meaning that safe practice should be followed in respect of record keeping and security.

- All users should also be aware that all email communications may be monitored at any time in accordance with the Acceptable Use Policy.
- Children are not permitted to send email communications, both outgoing and incoming messages.
- Users must report any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature. Aspects of online safety are shared with children and parents via Newsletters and our resources. Staff report to senior leaders within the school and can report to Lancashire directly.
- Users should be aware that they should not open attachments that they suspect may contain illegal content as they could inadvertently be committing a criminal act.
- All users must immediately report to the online safety champion/DSL any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature. If you are not satisfied with the response from the DSL and you feel it is a serious issue which has been downplayed or misunderstood, you can contact the NSPCC whistleblowing helpline and take the digital incident beyond the setting.
- The Federation have their own whistleblowing policy (updated LCC April 2025) and demonstrates a clear process of whistleblowing. Hard copies available on each school staff room board.
- Sophos Central is an anti-virus and threat protection service which provides schools with licences for a comprehensive suite of technologies to protect school devices from a wide variety of threats.

## **Social Networks**

Social Network sites allow users to be part of a virtual digital school community. They include sites such as Facebook, Instagram. These sites provide users with simple tools to create a profile or page including basic information about themselves, photographs, and possibly a blog or comments. As a user on a Social Network site, it may be necessary to access and view other users' content, send messages and leave unmediated comments.

Many Social Network sites are blocked by default through filtering systems used in schools, but these settings can be changed at the discretion of the head teacher.

Where social networking sites are used staff should always conduct themselves in a professional manner. If content is made available on the web it is available for everyone to see and potentially remains there forever.

All staff need to be aware of the following points:

- The content on Social Network sites may be unmediated and inappropriate for certain audiences.



- If a Social Network site is used personally, details must not be shared with children and privacy settings be reviewed regularly to ensure information is not shared automatically with a wider audience than intended.
- Staff must not give personal contact details to parents/carers including mobile telephone numbers, details of any blogs or personal websites; in line policies – social media and code of conduct.
- Staff are advised not to contact parents through social media sites applies to both current and ones attended setting in past.
- Any content posted online should not bring the school into disrepute or lead to valid parental complaints. It should not be deemed as derogatory towards the school and/or its employees or towards children and/or parents and carers. It should not bring into question the appropriateness of staff to work with children and young people. Follow this guidance along Social media policy and code of conduct.
- Online reputation should be at the forefront of your mind any time your post for setting or personal status.
- Online Communications with parents, past pupils or siblings of pupils, especially if under the age of 18 should be discouraged.
- Any digital concern of a member of the nursery community.... report to DSL.

### **Instant Messaging or VOIP**

Instant Messaging systems, e.g. Text messaging, Skype, Facetime, are popular communication tools with both adults and children. They can provide an opportunity to communicate in 'real time' using text, sound and video.

- Staff and children need to be aware of the risks involved using this technology e.g. viewing inappropriate images or making unsuitable contacts.
- Staff do not use school equipment to communicate with personal contacts e.g. through 'Facetime' on an iPad?
- Any communication, e.g. text messaging to contact parents, is to be kept secure and contact lists are stored securely in the school office.
- Various systems, e.g. CPOMS are being used regularly in schools as communication tools, secure access to a designated few are given.

### **Websites and other online publications**

This may include for example: school websites, Social Network profiles, podcasts and videos.

Information posted online is readily available for anyone to see and thus form an opinion about the school. From September 2012, the School Information (England) (Amendment) Regulations 2012 specified that certain up to date information must be made available on a school's website. More details regarding these requirements can be found on the DfE website or at


<http://www.legislation.gov.uk/ukxi/2012/1124/made>

- The school website is used as one method to communicate Online Safety messages to parents/carers via links to Online Safety sites and access to the Online Safety policy.
- From September 2023 at DS will be using a Linked in page to provide parents with a "one stop shop" for the online systems used within school admin processes (website; ParentPay for online payments and group call for text messaging and form completion).
- Everybody in the school who is involved in editing and contributing to the website, Facebook page and YouTube channel is made aware of the guidance for the use of digital media.
- Everybody in the school should also be aware of the guidance regarding the inclusion of personal information on the website. Staff and governing body to complete annual online safety training module via the National College.
- Editing online publications is restricted to staff who have the responsibility to ensure that the content is relevant and current.
- Overall responsibility for what appears on the website lies with the head teacher.
- A nominated governor undertakes a website self-review tool/paperwork which is feedback to the governor body at the next meeting
- **The online safety governance audit will be completed by a named Governor on:**

**In our obligation to "Keeping Children Safe in Education"** The self-review tools are:

**360degree safe**, an online safety self-review tool for schools. Every year, the data collected through the tool is analysed to see the common trends. <https://360safe.org.uk/>

**Project Evolve**, is a free toolkit that covers all aspects of the UKCIS "Education in a connected world" Framework, across all age phases from nursery to 18 years. <https://projectevolve.co.uk>

- Consideration is given to the use of any content subject to copyright/personal intellectual property restrictions.
- Downloadable materials in a read-only format (e.g. PDF) where necessary, to prevent content being manipulated and potentially re distributed without the school's consent.
-  Google Translate is now on the school website. (top right corner) Select your desired language from a dropdown list and the page instantly appears in that language. Whilst not perfect it is more than comprehensible and is getting better all the time. (Urdu, Bengali, French)
- YouTube is used for teaching if the page has already been checked beforehand.

- Duke Street Nursery School has a YouTube page; which was utilised to provide remote learning opportunities to families and children over the period of Covid lockdown 2020-2021.
- Children are not allowed to use YouTube themselves.
- Children are not allowed to use Facebook
- Web site photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.
- Pupils' full names will not be used anywhere on the Web site, particularly in association with photographs.
- Written permission by way of online forms which are completed at the beginning of the term through the induction from parents or carers will be obtained before photographs of pupils are published on the school Web site.

## Infrastructure and technology



# Anti-Virus and Threat Protection Service (Sophos Central)

## About the Service

The Anti-Virus and Threat Protection Service (Sophos Central) provides schools with licences for a comprehensive suite of technologies to protect your school's devices from a wide variety of threats. Sophos Central is a cloud-hosted security suite that provides schools access to modern security tools and protection.

This service includes licencing for the following features:

- Threat Protection (Anti-Virus) – Detection and automatic removal of ransomware, viruses and malware.
- Application Control – Block, allow or monitor Applications by category or name.
- Device Control – Block, allow or monitor removable media and peripherals such as USB sticks, Bluetooth or DVDs.
- Data Loss Prevention – Block, allow or monitor the transfer of confidential information from your ICT systems.
- Server Lockdown – Prevents unauthorised software from being installed on servers.

We will configure your school's service with the Threat Protection (Anti-Virus) configuration, you can then either use "as is" or customise to your school's needs by adding the other features.

## What are the benefits?

- Sophos Central can quickly detect and disinfect a wide range of threats.
- Your subscription will allow you to install the Sophos Central Intercept X Advanced or Sophos Central Intercept X Advanced for Server endpoint protection on each compatible device in your school.
- By protecting your ICT systems and data, you are helping to ensure your compliance with data protection requirements.
- Each school has access to their own Sophos Central Dashboard.
- Email alerting to schools in the case of outstanding events.
- Comprehensive reporting capability.
- The option to further secure devices by controlling the applications they run or the peripherals that connect to them.

School ensures that the infrastructure/network is as safe and secure as possible. Duke Street & Highfield Nursery School Federation are supported via an SLA with Education Digital services providing CLEO Secure Schools Network Broadband Service and so internet content filtering is provided by default. It is important to note that the filtering service offers a high level of protection, but occasionally unsuitable content may get past the filter service. Sophos Central is Anti-Virus and threat protection service to protect school devices from a wide variety of threats.

Web Filtering & Online Protection (Net sweeper) service enables safe web access. The web filtering is delivered through a Private Cloud, managed by Net sweeper. The cloud solution improves the performance of the filtering system and provides enhanced upgrade support.

**Netsweeper OnGuard** – this provides real-time Monitoring and Alerting system to provide online safeguarding for pupils. It can be used as a tool to quickly alert key schools' staff, such as designated safeguarding leads (DSLs).

## Broadband Network - Security Features

Our schools, broadband network is a private wide-area network (WAN), which is connected to the Higher Education JANET network and benefits from JISC CSIRT security benefits and features:



1. **Our broadband network firewall** is a network security device that monitors traffic to or from your network. It allows or blocks traffic based on a defined set of security rules.
2. **Security Monitoring:** JISC CSIRT provides extra security monitoring to help protect educational institutions in the UK.
3. **Incident Management:** Lancashire County Council Education Digital Services works with JISC CSIRT to manage any security incidents or risks identified, ensuring the safety of schools and students.
4. **DDoS Protection (Distributed Denial-of-Service):** Schools connected to our broadband network get additional protection against DDoS attacks, thanks to JISC CSIRT.
5. **Liaison:** In case of any cyber incidents, Lancashire County Council liaises with JISC CSIRT on behalf of the schools to handle the situation.

## Firewalls



Our broadband network firewall offers Dual ISP (Internet Service Provider) grade firewalls located at different data centres. These give excellent protection, performance and resilience.

Education Digital Net sweeper is the web filtering software and Sophos Central (Anti-Virus and Threat Protection Service) is a cloud-hosted security suite that provides schools access to modern security tools and protection.

## Anti-Virus and Threat Protection Service (Sophos Central)



The Anti-Virus and Threat Protection Service (Sophos Central) provides schools with licences for a comprehensive suite of technologies to protect your school's devices from a wide variety of threats. Sophos Central is a cloud-hosted security suite that provides schools access to modern security tools and protection.

## Web Filtering

**All our broadband connections include Web Filtering as standard. Based on Netsweeper, our service provides safe, filtered, and logged web access for both staff and students and is included in our [Broadband and Online Services bundle](#).**

- Education focused web filtering.
- Meets the DfE recommendations for web filtering to protect pupils online and the standards for schools' web filtering set by the UK Safer Internet centre.
- Different filtering policies based on username, group membership or IP range.
- Local control to allow your school to manage which websites and categories of websites it wishes to allow or block.
- Monitoring and reporting on web access.
- Illegal content (as listed on the Internet Watch Foundation) remains blocked at all times and access cannot be over-ridden by school staff.
- Provides filtered web access to all devices in school.
- Includes access to a reporting tool, schools can configure and schedule their own reports of internet usage via a number of templates.

### **Children's access – online risks in early years settings**

Content (what they see/encounter)

Contact (risk of someone communicating/video chat/live streaming)

Conduct (how we behave, respectfully, model behaviour, develop good habits; using for appropriate amount of time)

Commerce (any form of spending; encountering ads; providing an unrealistic view of the world; child will be unaware of their commercial behaviour).

- Children are always supervised when accessing school equipment and online materials (e.g. Working with a trusted adult). Use of the computers at break and during lunchtimes is prohibited unless in a supervised club.
- Children's access to the school systems by class/ general children's logins.
- Children's access is restricted to certain areas of the network and computer.

### **Adult access**

Access to school systems is restricted for all staff according to their areas of responsibility.

The role of the practitioner is to provide a positive attitude towards devices; direct lessons around online safety; modelling appropriate behaviours within the setting. Children are naturally curious; rich, real world experiences support learning and its vital practitioners promote use in a respectful way.

Other topics of online safety already identified earlier in the policy demonstrate the federation robust online safety approach to early years.

## **Passwords**

- All staff should be aware of the guidelines in the Lancashire ICT Security Framework for Schools. This is available at <https://educationdigitalservices.lancashire.gov.uk/support/security-and-safeguarding.aspx>
  - All adult users of the school network have a secure username and password. Password are changed every 60 days.
  - The administrator password for the school network are only available to Lynne Dickinson (at Duke Street); Claire Bland (Highfield) or the Educational Digital Services Technician.
  - Staff and children are reminded of the importance of keeping passwords secure.
  - Passwords can be changed at the individual's discretion by consultation with the ICT technician or Business Manager.
  - There is agreed format for creating passwords for adults e.g. mixture of letters, numbers and symbols.
- 
- School has legal ownership of all software (including apps on tablet devices).
  - School keeps an up-to-date record of appropriate licenses for all software. Full details are held with Education Digital Services.
  - An annual audit of equipment and software is made.
  - The ICT technician and the head teacher control what software is installed on school systems.
- Managing the network and technical support
- Any servers, wireless systems and cabling are securely located and physical access is restricted.
  - All wireless devices have been security enabled.
  - All wireless devices are accessible only through a secure password.
  - Relevant access settings should be restricted on tablet devices e.g. downloading of apps and purchases.
  - Education Digital services are responsible for managing the security of your school network. Monitored by LCC.
  - School systems are centrally managed via Sophos Central Dashboard for endpoint protection. Computers are regularly updated with critical software updates/patches and Sophos Central antivirus software is automatically updated.
  - Users (staff, children, guests) have clearly defined access rights to the school network e.g. They have a username and password and, where appropriate, permissions are assigned.
  - Staff and children are reminded to lock or log out of a school system when a computer/digital device is left unattended.



- Users are not allowed to download executable files or install software. The ICT Technician and Business Manager possess administrator rights and are responsible for assessing and installing new software.
- Users can report any suspicion or evidence of a breach of security to the ICT Technician and Business Manager or the head teacher.
- No longer working ICT equipment to be disposed of following guidance from the LCC Education Digital services.
- School equipment, such as teacher's laptops or cameras, should not be used for personal/family use.
- Any network monitoring takes place in accordance with the Data Protection Act (2018). Staff are told that the network may be monitored from time to time.
- All staff are aware of the contents of this policy and aware of the standards required to maintain Online Safety in the school.

### **Filtering (Netsweeper) and virus protection (Sophos Central)**

- Duke Street & Highfield Nursery School Federation uses Netsweeper
- **Prevent Duty**, Netsweeper is complying with the Government's current Prevent Duty guidance.
- Full school SLA with Education Digital Services
- Information regarding devolved filtering, is communicated if necessary to members of staff through staff meetings and via email. Staff wishing to block or unblock websites may do so by making a request to Education Digital Services.
- Staff that take laptops home are required to connect to school systems when back on site to ensure that all updates are updated regularly.
- Staff report any suspected or actual computer virus infection directly to Education Digital Services via the "incident log" on the school portal.

## **Dealing with incidents**

Incidents are reported to the Head teacher/Education Digital Services on their half termly visits.

Any suspected illegal material or activity must be brought to the immediate attention of the head teacher who must refer this to external authorities, e.g. Police, CEOP's or the Internet Watch Foundation (IWF). Never personally investigate, interfere with or share evidence as you may inadvertently be committing an illegal offence. It is essential that correct procedures are followed when preserving evidence to protect those investigating the incident.

Always report potential illegal content to the Internet Watch Foundation (<http://www.iwf.org.uk>). They are licensed to investigate – schools are not! Examples of illegal offences are:

- Accessing child sexual abuse images
- Accessing non-photographic child sexual abuse images
- Accessing criminally obscene adult content
- Incitement to racial hatred

### **Web filtering (Netsweeper) onguard**

onGuard is a Digital Safety Monitoring system.

onGuard is Netsweeper's premier student protection product.

OnGuard monitors all activity on computers, and can alert DSL:

(Designated Safeguarding Lead) to potential risks such as:

- Cyber-bullying
- Self-harm
- Grooming
- Terrorism

Detected alerts can be viewed by your DSL on a web-accessible dashboard.

Any computer activity which initiates an alert; onguard will:

- Take a screenshot, and upload this to the onGuard dashboard with details of the user, the computer and time it occurred.
- Automatically categorise the alert. If it believes there is a threat of harm to a person, this will alert the Netsweeper onGuard team (staffed 24/7). If this is verified as a likely threat, the onGuard team will call the (pre-registered) school contacts. If they cannot make contact, and if the school have authorised this, the onGuard team will call the police.
- The DSL will receive email notification of any alerts (these can be configured to provide daily emails), and can review the schools' onGuard dashboard to acknowledge alerts and make notes on individual cases.

To accurately determine who is at risk, onGuard uses active system monitoring, including optical character recognition, to detect user activity and send alerts if potential risks are identified.

### **Inappropriate use**

It is more likely that school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with quickly and actions are proportionate to the offence.

## Incident Procedure and Sanctions

In the event of accidental access to inappropriate materials;

Minimise the webpage/turn the monitor off. Tell a trusted adult.

- Inform the school Business Manager; access for evidencing the Netsweeper onguard summary. Further details to be reported to the Headteacher and the governing body.

If other people's logins and passwords are used maliciously, inappropriate materials are searched for deliberately, inappropriate electronic files are brought from home or chat forums are used in an inappropriate manner;

- Inform Education Digital Services immediately.
- Inform the school business manager.
- Enter the details in the Incident Log.
- Implement additional Online Safety training with the individual child or class.
- Take appropriate action in relation to the disciplinary policy, e.g. contact parents.

## Responding to Misinformation, Disinformation and Conspiracy Theories

As part of our safeguarding responsibilities, the school recognises the risks posed by misinformation, disinformation, and conspiracy theories online. These can undermine children's understanding of the world, expose them to harmful narratives, and affect their wellbeing.

### School Response

- **Filtering and Monitoring:** Our Onguard system is configured to detect and restrict access to known sources of misinformation and harmful content. Alerts are reviewed by safeguarding staff to ensure appropriate action is taken.
- **Curriculum Integration:**
  - For nursery and EYFS children, teaching is age-appropriate and focuses on developing critical thinking, curiosity, and trust in reliable adults.
  - Stories, play, and guided discussions are used to help children distinguish between "real" and "pretend," laying the foundation for understanding truth and reliability.
  - Staff model safe online behaviours and encourage children to ask questions if they encounter confusing or worrying information.

- **Parental Engagement:** Parents are informed about the risks of misinformation and disinformation and are supported with guidance to reinforce safe practices at home.

## **Governors' Oversight**

Governors are responsible for ensuring that:

- The Online Safety Policy explicitly addresses misinformation, disinformation, and conspiracy theories.
- Staff are trained to recognise and respond to these risks in ways appropriate to the age and stage of the children.
- Curriculum planning includes opportunities to build resilience and critical awareness in early years.
- Safeguarding reports to governors include updates on how these risks are being managed.

## **Acceptable Use Policy (AUP)**

The Acceptable Use Policy is intended to ensure that all users of technology within school are responsible and are protected from potential risk in their everyday use of ICT for educational, personal and recreational purposes.

The AUP is provided for Staff, Children and Visitors/Guests and to be adhered to by users before access to technology is allowed. The parental agreement is a partnership between parents/carers, children and the school to ensure that users are kept safe when using technology. A list of children who, for whatever reason, are not allowed to access technology will be kept in school and made available to all staff.

Staff have responsibility for school ICT equipment that they have ownership of as well as classroom equipment which they are supervising the use of.

The AUP reflects the content of the school's wider Online Safety Policy and is regularly reviewed and updated. It is regularly communicated to all users and is understood by each individual user and relevant to their setting and role/ responsibilities.

Staff are advised to fully read and understand the terms of the following policies within schools. *Note these are updated annually following Kcsie annual updates, GSWP and other LCC updates and Dfe Guidance*

- 1) Online safety policy
- 2) Safeguarding policy
- 3) Code of conduct

## Education and training

In 21st Century society, both adults and children need to be digitally literate and aware of the benefits that use of technology can provide. However, it is essential that children are taught to use technology responsibly, securely and safely, being able to recognise potential risks and knowing how to respond. They should, for example, be able to communicate safely and respectfully online, be aware of the necessity to keep personal information private, be taught how to search effectively and be discerning in their evaluation of digital content and be aware of the need to respect copyright and Intellectual Property rights.

The three main areas of Online Safety risk (as mentioned by OFSTED, 2013) that need particular consideration are;

### Content

Children need to be taught that not all content is appropriate or from a reliable source.

Examples of risk include;

- Exposure to inappropriate content, including online pornography, ignoring age ratings in games (exposure to violence associated with often racist language) and substance abuse
- Lifestyle websites, for example pro-anorexia/self-harm/suicide sites
- Hate sites
- Content validation: how to check authenticity and accuracy of online content
- Protecting against illegal, inappropriate or harmful content online.

### Contact

Children need to be taught that contact may be made when using digital technologies and that appropriate conduct is necessary when engaging with these technologies. Examples of risk include:

- Grooming
- Cyberbullying in all forms
- Identity theft (including 'fraud' – hacking Facebook profiles) and sharing passwords
- Safeguarding against risks associated with online interactions.

## Conduct

Children need to be made aware that their personal online behaviour can increase the likelihood of, or cause harm to themselves or others. Examples of risk include:

- Privacy issues, including disclosure of personal information, digital footprint and online reputation
- Health and well-being – amount of time spent online (internet or gaming)
- Sexting (sending and receiving of personally intimate images)
- Copyright (little care or consideration for intellectual property and ownership – such as music and film).
- Promoting respectful and responsible online behaviour.

**Commerce**\_- any form of spending/encountering ads/risk of in app purchases. Preventing risks from online gambling, phishing and financial scams.

These principles are part of the statutory guidance for schools in England, KCSIE which aims to equip educators with a systematic method to identify and manage online risks.

***Due to the age of our children, the above messages will be given to parents and only taught to children in an age appropriate way if applicable.***

Staff training requirement – access cyber security module and further understanding on AI threats; all available on National College

## Online Safety- Across the curriculum

It is vital that children are taught how to stay safe, protect themselves from harm and take a responsible approach to their own and others' online safety. Barden provides relevant, flexible and engaging Online Safety education to all children as part of their curriculum entitlement.

- Online Safety education is progressive throughout the year. Staff are provided with a list of suitable sites, resources and activities for early years.
- Duke Street & Highfield Nursery School Federation takes part in the annual 'Safer Internet Day' activities that focus on Online Safety during the National Online Safety Awareness Week.
- The role of practitioners is to demonstrate a positive attitude towards devices and direct lessons around online safety and modelling appropriate behaviours within the setting. By equipping practitioners with awareness and training on the importance of online safety; responsible technology use and how to identify the signs of

inappropriate behaviour we are equipping practitioners with knowledge and skills to demonstrate our commitment to online safety. .

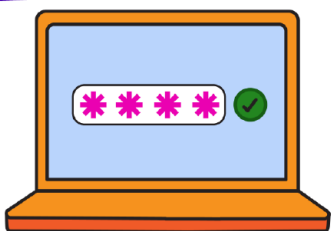
- As part of the Online Safety training parents are made aware of the impact of cyberbullying and how to seek help if they are affected by these issues, e.g. encouraging their children to talk to a trusted adult in school or parent/carer.
- Collaboration with parents is crucial. We communicate our approach to online safety and provide guidance through monthly newsletters; providing guidance/tips from National Online Safety.
- At home visit with new starters; staff are encouraged to utilise the home visit to understand how technology is used in the home to inform your approach to teaching and to promote online safety.
- Schools within the federation participate in the #WakeupWednesday; [National Online Safety | News | National Online Safety](#) amongst other information a new platform guide is shared weekly which we can share with parents.
- Parents are provided with regular updates/online leaflets around [Digital Parenting - Vodafone UK News Centre](#);

### **Online Safety– Raising staff awareness**

- Online Safety is a fixed item on staff meeting agendas and discussed at each meeting and during Inset time.
- Annual certificate in Online safety for staff for nurseries is to be completed through the National College portal and completed Sept each year.
- Other Online Safety training can be provided in school or from external agencies such as Lancashire advisory service and the police. (CEOP)
- [Keeping children safe online | NSPCC](#)
- Online Safety training/discussions/annual updates/full staff induction ensure staff are made aware of issues which may affect their own personal safeguarding e.g. use of Social Network sites.
- All staff are expected to promote and model responsible use of ICT and digital resources.
- Online Safety training is provided within an induction programme for all new staff to ensure that they fully understand both the school's Online Safety Policy and Acceptable Use Policy.
- The Online Safety Policy, Acceptable Use Policy, curriculum resources and general
- Staff are required to sign annually Acceptable User Agreement/staff code of conduct for ICT (Appendix 1)

# Cyber Aware

Advice on how to stay secure online.



## Actions to improve your cyber security

Most of us are spending more time online. So it's important to secure the **personal information** we store on the internet, and the **devices** we use to access this information.



## Improve your password security

Passwords are the gateway to your online accounts. Here are three actions to ensure your passwords are working hard to protect your personal and financial information.

### 1 Create a unique password for your email account

If a cyber criminal accesses your email, they can use it to reset all your other account passwords (and get access to all your other accounts). This is why it's important to create a strong password for your email account, and make sure it's different to all your other online passwords.



### 2 Create strong passwords using three random words

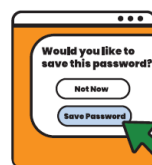


Cyber criminals can easily guess weak, short passwords. You can quickly make a strong password by combining three random words to create a single password (for example **PuddingTorchPizza**). If you're asked to include special characters when creating a password, you can include them in your three random words (for example **PuddingTorchPizza!**).

### 3 Save passwords in your browser

Most web browsers (such as Chrome, Safari and Edge) will offer to save your passwords for you. It's safe for you to do this.

Letting your browser do this means you can use unique, strong passwords for **all** your important accounts (rather than using the same password for all of them, which you should never do).

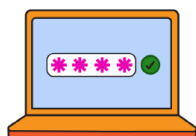


## Add extra protection

Now you've got your passwords sorted, you're ready to take cyber security to the next level.

### 4 Turn on 2-step verification (2SV)

Turning on 2SV will stop criminals getting into your account, even if they know your password. 2SV (also known as **2-factor authentication**, or **multi-factor authentication**) simply means you'll be prompted for a second piece of information when signing into your account. This is usually a code which will be sent via text or email.



### 5 Update your devices

You should update your apps and your device's software when you're prompted. Updates include protection from viruses and will often include new features. Applying these updates is one of the most important (and quickest) things you can do to keep yourself safe online. You can make things even safer by turning on **automatic updates**.

## Back up your photos, documents, and other personal data

Congratulations! If you've followed these actions, you're protected from the vast majority of cyber attacks. But if something does go wrong, backing up means you will always have access to your important data.

### 6 Make sure your important data is backed up

A backup is a copy of your important data such as photos, documents, and other personal data stored on your IT equipment. Once you've made a backup, if you lose access to your original data, you can restore a copy of it from the backup.

If you use products from Apple, Google or Microsoft (such as Windows computers, Apple and Android phones and tablets), you'll be able to back up your data to the internet. Check your devices to see **what** is being backed up, **how** often, how much **data** you're allowed, and that **automatic backups** is switched on.

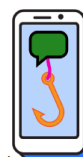
## Report suspicious messages

By reporting suspicious messages, you'll be helping to prevent others becoming victims of cyber crime.

### 7 Report suspicious messages

If you've received a suspicious email or text message that doesn't feel right, or visited a scam website, don't panic.

- Forward suspicious texts to 7726
- Forward suspicious emails to [report@phishing.gov.uk](mailto:report@phishing.gov.uk)
- Report scam websites to the NCSC by visiting: [nsc.gov.uk/report-scam-website](https://nsc.gov.uk/report-scam-website)
- If you think you've been a victim of fraud, contact your bank immediately and report it to Action Fraud online at [actionfraud.police.uk](https://actionfraud.police.uk) or by calling 0300 123 2040
- If you live in Scotland, report all fraud (and any other financial crime) to Police by calling 101



For more information on how to get secure online visit [cyberaware.gov.uk](https://cyberaware.gov.uk). If you're a sole trader or a small business you can also find bespoke advice there.



## Online Safety– Raising parents/carers awareness

"Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on



the internet and are often unsure about what they would do about it.” (Byron Report, 2008).

From information already provided the school offers opportunities for parents/carers and the wider community to be informed about online safety, including the benefits and risks of using various technologies both at home and at school through:

- School newsletters, School Website and other publications
- #Wake up Wednesdays
- Promotion of external Online Safety resources/online materials from NOS
- Online safety and other information is provided to parents and carers via the school website and other sharing platforms; ie. Tapestry

### **Facebook**

The following staff administer on Facebook and monitor content – Sue Conron, Natalie Sinclair, Louise Phillips, Sam Offord, Laura Erskine, Gemma Devlin.

### **Facebook**

The following staff administer on Facebook and monitor content – Claire Bland, Leah Pickering, Claire Murray, Natalie Sinclair, Sue Conron (HF).

Louise Phillips, Sue Conron, Gemma Devlin, Sam Stringfellow (DS)

### **Instagram**

The administrator is Laura Erskine and monitors content.

### **Online Safety– Raising Governors’ awareness**

All governors complete annually the certificate for online safety for Governors via The National College, particularly those with specific responsibilities for online safety, ICT or child protection, are kept up to date through discussion at Governor meetings, head teachers report, attendance at Local Authority Training, CEOP or internal staff/parent meetings.

NB: The Online Safety Policy is reviewed and approved by the governing body.

### **Evaluating the impact of the Online Safety Policy**

By prioritising and implementing robust measures we can create a secure environment where children can benefit from technology within education whilst meeting requirements and expectations of Ofsted inspections.

There is a need to monitor and evaluate the impact of safeguarding procedures throughout the school. The head teacher and SMT are responsible

for the monitoring and evaluation of safeguarding (including online safety) within Federation of Duke Street & Highfield Nursery School. Individual staff are responsible for the recording and reporting of incidents

When monitoring takes place the school should consider:

- Is the Online Safety Policy is having the desired effect?
- Are Online Safety incidents monitored, recorded and reviewed effectively?
- Is the introduction of new technologies risk assessed?
- Are these assessments included in the Online Safety Policy?
- Are incidents analysed to see if there is a recurring pattern e.g. specific days, times, classes, groups and individual children and how can these patterns be addressed most effectively e.g. working with a specific group, class assemblies, reminders for parents?
- How does the monitoring and reporting of Online Safety incidents contribute to changes in policy and practice?
- How are staff, parents/carers, children and governors informed of changes to policy and practice?
- AUP updated? Current trends and technologies reviewed?

#### Updates for KCSIE 2025 Compliance

In alignment with the Keeping Children Safe in Education (KCSIE) 2025 guidance, the following updates have been incorporated into the Federation Online Safety Policy:

- Expanded '4 Cs' Framework: The policy now includes risks associated with misinformation, disinformation, and conspiracy theories under the 'Content' category.

- AI Risks and Guidance: Staff are trained to understand the implications of generative AI technologies. The policy includes measures to ensure safe and ethical use of AI in educational settings.

- DfE Self-Assessment Tool: The Federation will utilise the Department for Education's 'Plan Technology for Your School' self-assessment tool to evaluate and improve filtering and monitoring systems.

- Staff Training: All staff will receive updated training to identify and respond to emerging online risks, including misleading content and AI-generated misinformation.

- Policy Integration: Online safety measures are now embedded across safeguarding, curriculum, and IT policies. Annual reviews will ensure alignment with the latest KCSIE guidance.

- Terminology Updates: Language used in the policy has been updated to reflect current standards, including replacing outdated terms such as 'Autism Spectrum Disorder' with 'Autism'.