

Growing Together Federation

Bowerdean Nursery School
Henry Allen Nursery School
Mapledean Nursery School

E-SAFETY

Contents

2.1 Writing and reviewing the e-safety policy	3
2.2 Teaching and learning	3
2.2.1 Why the Internet and digital communications are important	3
2.2.3 Internet use will enhance learning	3
2.3 Managing Internet Access	3
2.3.1 Information system security	3
2.3.2 E-mail and Pupils	3
2.3.3 E-mail and Staff	4
2.3.4 Published content and the school web site	4
2.3.5 Publishing pupil's images and work	4
2.3.6 Social networking and personal publishing	4
2.3.7 Managing filtering	5
2.3.8 Managing mobile phones	5
2.3.9 Managing the taking and printing of pupil photographs	5
2.3.11 Managing emerging technologies	6
2.3.12 Protecting personal data	6
2.4 Policy Decisions	6
2.4.1 Authorising Internet access	6
2.4.2 Assessing risks	6
2.4.3 Handling e-safety complaints	6
2.4.4 Community use of the Internet	7
2.5 Communications Policy	8
2.5.1 Introducing the e-safety policy to pupils	8
2.5.2 Staff and the e-Safety policy	8
2.5.3 Enlisting parents' and carers' support	8
2.5.4 Tapestry software	8
Glossary	9
Tapestry Privacy Policy	10

2.1 Writing and reviewing the e-safety policy

The e-Safety Policy relates to other policies including those for ICT, bullying and for child protection.

The school will appoint an e-Safety Coordinator. This may be the Designated Child Protection Coordinator as the roles overlap. It is not a technical role.

Our e-Safety Policy has been written by the school, building on the Bucks e-Safety Policy and government guidance. It has been agreed by senior management and approved by governors.

2.2 Teaching and learning

2.2.1 Why the Internet and digital communications are important

The Internet is an essential element in 21st century life for education, business and social interaction. Nursery school age children are quite likely to have already accessed age appropriate internet sites in their homes. Children will only use the internet to access any sites at the nursery school under adult supervision and will be directly related to finding something out.

2.2.3 Internet use will enhance learning

The school Internet access will be designed expressly for child use, (under staff supervision only) and will include filtering by the service provider appropriate to the age of the children.

2.3 Managing Internet Access

2.3.1 Information system security

School ICT systems security will be reviewed regularly.

Virus protection will be updated regularly.

Security strategies will be discussed with the Buckinghamshire Council Advisors.

Personal data sent over the Internet will be encrypted or otherwise secured.

2.3.2 E-mail and Children

Due to the age of the children there will be no child access to e-mail.

2.3.3 E-mail and Staff

Staff are only to initiate contact with parents/carers for professional reasons and in agreement with parents/carers that they are happy to communicate via e-mail. All e-mail communication by staff with parents/carers must be by prior agreement with the head teacher.

Staff are only to use the .bucks.sch.uk for such emails.

2.3.4 Published content and the school web site

Staff personal or bucks.sch.uk contact information will not be published. The contact details given online should be those used by the school office only.

The head teacher and the web site manager will take overall editorial responsibility and ensure that content is accurate and appropriate.

The website should comply with the school's guidelines for publications including respect for intellectual property rights and copyright.

2.3.5 Publishing children's images and work

Photographs that include children will be selected carefully so that individual children cannot be identified or their image misused. Wherever possible, group photographs of children will be used.

Children's names will not be used anywhere on a school Web site or other on-line space, particularly in association with photographs.

Written permission from parents or carers will be obtained and kept on file before photographs of any child is published on the school Website.

Work can only be published with the permission of the child and parents/carers.

Parents should be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories

2.3.6 Social networking and personal publishing

The school will block access to any social networking sites. Staff using social networking sites outside of the nursery should never post or enter into dialogue regarding any information about the Growing Together Federation.

Staff should not be friends with parents of children at the Nursery School. Staff should not publish any information relating to the Nursery online.

2.3.7 Managing filtering

The school will work with the Buckinghamshire Council ICT team to ensure systems to protect children are reviewed and improved.

If staff or pupils come across unsuitable on-line materials, the site must be reported to the head teacher, who will ensure a report is made to the computer services provider.

Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

2.3.8 Managing mobile phones

Due to the ages of the children it is unlikely that any child will bring in a mobile phone but should this happen the phone will be removed and the parent/carer contacted to let them know we have the phone. (This is because it is likely to be a parent/carer's phone or possibly an older sibling).

Staff may use their own mobile phones to contact school when off the school premises. Mobile phones are not to be used to capture photographs of children at any time.

Staff will not use their mobile phone during the time pupils are on site except in an emergency and then only in the nursery school office. Staff mobile phones will be kept in the staff room or office.

All visitors to the site will be advised they may not use a mobile phone except in the nursery school office and may be asked to leave the site if they do not comply with this directive. If visitors are to be left unattended in the Nursery, their mobile phones will be taken and kept in a safe place in the office.

2.3.9 Managing the taking and printing of pupil photographs

Photographs taken by staff to support child learning or as a record of school events, e.g. History Days, sports events, or a child's learning activity, should only be taken using school digital cameras. No images are to be taken on personal digital cameras. Images can only be downloaded onto the school server and at no time can they be stored on home based laptops or computers.

All printing of child images by staff must be done on school printers. No images should be sent to a third party for printing except in the case of professional printing being required for example printing the nursery school prospectus. Parent/carer agreement would be sought for professional printing such as the prospectus. These images will be downloaded weekly onto the school computer, and deleted from the cameras.

For internal school events, e.g. Nativity, school visits or particular celebrations, parents will be allowed to take photos or videos of their own children. If parents wish to take a group photo, and there is a child present who has not consented to photos being taken, the child will be discretely removed, and parents can then take the photo.

Parents will be reminded that they must not share any photos of other children on media websites.

2.3.11 Managing emerging technologies

Emerging technologies will be examined for educational benefit by the senior management team and a risk assessment will be carried out before use in school is allowed.

No games machines (including the Sony Play station, Microsoft Xbox and others) are to be brought into Nursery at any time.

2.3.12 Protecting personal data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

2.4 Policy Decisions

2.4.1 Authorising Internet access

All staff must read and sign the 'e-safety Code of Conduct for ICT' before using any school ICT resource.

The school will maintain a current record of all staff and children who are granted access to school ICT systems.

Access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.

Parents will be asked to sign and return a consent form for child access to the internet.

Any person not directly employed by the school will be asked to sign an 'Acceptable use of school ICT resources' before being allowed to access the internet from the school site.

2.4.2 Assessing risks

The Growing Together Federation staff will take all reasonable precautions to prevent access to inappropriate material and all internet access will be supervised by a member of staff. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the school network, but would be immediately closed down by the supervising adult.

The school will audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate and effective.

2.4.3 Handling e-safety complaints

Complaints of Internet misuse will be dealt with by the Head teacher.

Any complaint about staff misuse, based on the e-safety Code of Practice, must be referred to the Head teacher.

Complaints of a child protection nature must be dealt with in accordance with the school child protection procedures.

Parents/carers will be informed of the complaints procedure (see school's complaints policy).

2.4.4 Community use of the Internet

The school will be sensitive to Internet related issues experienced by children out of school, e.g. social networking sites, (generally because of their young age social networking site experience this is likely to be via older siblings or parents/carers), and offer appropriate advice.

2.5 Communications Policy

2.5.1 Introducing the e-safety policy to pupils

e-Safety training will be embedded through reminders appropriate to the age of the children.

2.5.2 Staff and the e-Safety policy

All staff will be given the School e-Safety Policy and its importance explained.

Staff should be aware that network and Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

Staff that manage filtering systems or monitor ICT use will be supervised by the Head teacher and work to clear procedures for reporting issues.

Staff will always use a child friendly safe search engine when accessing the web with children.

2.5.3 Enlisting parents' and carers' support

Parents' and carers' attention will be drawn to the School e-Safety Policy in newsletters, the school brochure and on the school Web site.

The school will ask all new parents/carers to sign an e-safety agreement or Social Media Use Agreement when their child joins the Nursery.

2.5.4 Tapestry or ClassDojo – safe use of electronic online learning journal

Electronic records of children's learning including photographs are securely stored on Tapestry or ClassDojo. Staff have access to children's records via nursery tablets and secure login. Staff are able to access this securely at Nursery or from home, should they wish. Information is password protected and passwords must not be shared with anyone other than employees of the Growing Together Federation. When a member of staff leaves, the passwords must be re-generated to prevent future unauthorised access.

For further information please refer to the Tapestry or ClassDojo privacy policy attached.

Glossary

Acceptable use policy (AUP)	A policy that a user must agree to abide by in order to gain access to a network or the internet. In the schools context, it may also cover how other communications devices, such as mobile phones and camera phones, can be used on the school premises.			
ALT tag	ALT tags, or alternate text tags, are typically used to provide further detail on an image on a web page. The text is seen when the image is being loaded, and is also often seen when a mouse is passed over the image.			
Blog	A blog, also known as a weblog, is a form of online diary or journal. Blogs contain short, frequently updated posts, arranged chronologically with the most recently posted item appearing at the top of the page. In addition to text, blogs can contain photos, images, sound, archives and related links, and can incorporate comments from visitors.			
Bluetooth	Bluetooth is a telecommunications industry standard which allows mobile phones, computers and PDAs to connect using a short-range wireless connection.			
Bookmarking	The process of storing the address of a website or internet document on your computer, so that you can find it again easily.			
Caching	The process of temporarily storing files, such as web pages, locally to enable quick access to them in the future without placing demands on network resources.			
Chatroom	An area on the internet or other computer network where users can communicate in real time, often about a specific topic.			
Digital video	Video captured, manipulated and stored in a digital format.			
Filtering	A method used to prevent or block users' access to unsuitable material on the internet.			
Firewall	A network security system used to restrict external and internal traffic.			
Hacking	The process of illegally breaking into someone else's computer system, breaching the computer's security.			
Information and support (ICT) teachers, learning and Communications	The computing and communications facilities and features that, in an	Technologies	educational	context, variously range of activities.
Information literacy	The ability to locate pertinent information, evaluate its reliability, analyse and synthesise it to construct personal meaning and apply it to informed decision making.			
Internet service provider (ISP)	A company providing a connection to the internet and other services, such as browser software, email, a helpline, webspace and subscriber-only content.			
Personal digital too. assistant (PDA)	A small, mobile, handheld device that provides computing and information storage/ retrieval capabilities, and possibly phone facilities			
Spam	Unsolicited junk email. The term is also used to describe junk text messages received via mobile phones. A related term, spim (or splm), describes receiving spam via instant messaging.			
Trojan horses	A virus which infects a computer by masquerading as a normal program. The program contains additional features added with malicious intent. Trojan horses have been known to activate webcams, for example, without the knowledge of the PC user.			
Video conferencing	The process of conducting a conference between two or more participants over a network, involving audio and often text as well as video.			
Virus	A computer program which enters a computer, often via email, and carries out a malicious act. A virus in a computer can corrupt or wipe all information in the hard drive, including the system software. All users are advised to guard against this by installing anti-virus software.			
Webcam	A webcam is a camera connected to a computer that is connected to the internet. A live picture is uploaded to a website from the camera at regular intervals, typically every few minutes. By looking at the website you can see what the camera sees – almost as it happens.			

Tapestry Privacy Policy

This privacy policy is for the users of the Tapestry online learning journal service, (<https://tapestryjournal.com>), which is owned and operated by The Foundation Stage Forum Ltd., (<http://evfs.info>). In the document below, 'We' means The Foundation Stage Forum Ltd.

The Foundation Stage Forum Ltd is registered with the [UK Information Commissioners Office](#), reference Z1783069.

The Service

Schools and nurseries pay The Foundation Stage Forum to provide them with a service that allows them to create online learning journals for children under their care and to share them with their staff and, if the school or nursery wishes, the children's parents and relatives.

What data do we collect?

For each school or nursery, we store:

- The name and address of the school or nursery
- The name, email address and telephone number of the person at the school or nursery who pays for our service.

We store this information in order to administer and charge for our service.

The school or nursery may then store some or all of the following data on our service:

- The names and email addresses of their staff
- The names, dates of birth and addresses of their children
- The names and email addresses of the parents and relatives of their children
- The contents of a learning journal:
 - assessments of children's performance
 - notes, photographs and videos of the children

The school or nursery stores this information in order to record, analyse and, if they wish, share the progress of their children. The school or nursery has the freedom to choose which of the above data they store, and are able to delete it at will. The school or nursery choose who has access to the data.

In providing the service, we will send automated emails to staff and parents in order to confirm email addresses, reset passwords and notify them of events relating to the school or nursery (such as when a new observation is added about a child). We never send any marketing information, though we do send staff a newsletter about Tapestry.

We ONLY access the data stored by the school or nursery about staff, children or relatives when we have to in order to maintain the service to the school or nursery, or to fix faults.

We collect the following information from visitors to our sites:

- IP addresses
- Information about their web browser and computer
- What pages people look at (e.g., the list of observations), but not the content of those pages (i.e., we could not tell directly from the data whether the list of observations contained information about a particular child, though given time and access to the data above it would be possible to figure that out)

We use this information to monitor the security of our service, to help us figure out how to improve the service (e.g., what browsers should we support? how much capacity should we add?) and to improve the way we market the service (e.g., what search terms were used to discover our site).

We collect the following information from users of our phone and tablet applications:

- The make and model of the device
- The version of the operating system
- Details of any crashes that occur in the application
- What screens people look at in the application (e.g., the list of observations), but not the content of those screens (i.e., we could not tell directly from the data whether the list of observations contained information about a particular child, though given time and access to the data above it would be possible to figure that out)

We use this information to help us figure out how to improve the service (e.g., what causes crashes? which crashes need fixing most urgently?)

We collect the following information about people who contact us by email or through our support ticket system:

- The person's email address and the contents of the email

We use this information to respond to questions or problems raised by our users.

When people pay for our services, we pass them to a Payment Service Provider (PSP), currently SagePay who will collect the appropriate credit card and address verification details. We do not hold any of that information ourselves.

Who owns the data?

The school or nursery own the data they place in our service. We do not. Formally, in ICO terms, the school or nursery are the "Data Controller" and we are the "Data Processor".

Who do we share data with?

We do not share data, except as explicitly requested by the school or nursery.

If they wished, the school or nursery might give staff, parents or relatives access to data. They might download or print some or all of the data and share it with their staff, parents or the government. They might transfer some of the data to a different nursery that uses Tapestry.

We, the Foundation Stage Forum Ltd, ONLY access the data stored by the school or nursery in order to carry out the school or nursery's instructions, to maintain the service to the school or nursery, or to fix faults.

How do we collect the data?

Most of the data is entered by the staff at the nursery or school directly into our website or through our phone and tablet applications. The nursery may, if they wish, permit parents and relatives of children to add data to the service.

We store cookies on users' computers in order to verify that the user is logged in and to store their preferences. The cookies themselves do not contain any identifiable information about the user or about what they are looking at.

The information about the computers that visit our site is collected by Google Analytics. No information that is stored by the school or nursery on our system is sent to Google (i.e., Google doesn't get to see anything about the staff, parents or children). You can read Google's privacy policy here: <https://support.google.com/analytics/answer/6004245?hl=en>

The information about the make and models phones and tablets that use our applications and the crash reports from when our app crashes is collected by Crashlytics. No information that is stored by the school or nursery on our system is sent to Crashlytics (i.e., Crashlytics doesn't get to see anything about the staff, parents or children children). You can read the Crashlytics privacy policy here: <https://try.crashlytics.com/terms>

Payment information is given directly to a Payment Service Provider (PSP), currently SagePay. We do not hold any financial information ourselves.

Can I have my data corrected or deleted?

Yes. The school or nursery can correct or delete the data they store about their staff, children or parents.

The school or nursery can correct the information we store about them through their Foundation Stage Forum account. They can also contact us and we will correct or delete it on their behalf.

The process of deletion is gradual: initially deleted data is moved to a 'deleted' area in case it was deleted in error. After a delay, it is then permanently deleted from our main systems. After a further delay, it is then permanently deleted from our backups.

What are the school or nursery's responsibilities?

The school or nursery that uses our service has overall responsibility for complying with the Data Protection requirements (or the equivalent in other countries).

When they take out a Tapestry subscription, they agree to our terms and conditions, which are available from within the Tapestry control panel at any time.

It is important that the school or nursery have taken care to:

- Think about what information it is appropriate to share with whom, given their situation and that of the children under their care.
- ;Ensure they have permission from parents or carers for the data they store about them and the way that they use that data.
- Train their staff about sensible security and confidentiality precautions:

- Taking care of passwords
- Taking care not to install software on computers that may compromise security.
- Taking care not to access material from inappropriate places where it can't be kept appropriately confidential.
- Prevent access to Tapestry for parents whose children have been made inactive or have been deleted, unless they have other children at your setting.
- Give parents instructions for keeping the data protected, e.g. by insisting no photos are uploaded to social media sites without the written permission of the parents whose children are depicted in photos, videos or text.

ClassDojo Privacy Policy

[Privacy Policy | ClassDojo](#)