Acceptable Use and E-safety Policy

Kingsway Primary School

Covid adaptation

Governor Committee Responsible:	Business and Finance	**Staff Lead**:	Dan Cox
Status	Non-statutory	**Review Cycle**	Annual
Last Review	January 2021	**Next Review Date**	End of Covid or September 2021

1. Introduction and aims

ICT is an integral part of the way our school works, and is a critical resource for pupils, staff, governors, volunteers and visitors. It supports teaching and learning, pastoral and administrative functions of the school.
However, the ICT resources and facilities our school uses also pose risks to data protection, online safety and safeguarding.

This policy aims to:

- Set guidelines and rules on the use of school ICT resources for staff, pupils, parents and governors
- Establish clear expectations for the way all members of the school community engage with each other online
- Support the school’s policy on data protection, online safety and safeguarding
- Prevent disruption to the school through the misuse, or attempted misuse, of ICT systems
- Support the school in teaching pupils safe and effective internet and ICT use

This policy covers all users of our school’s ICT facilities, including governors, staff, pupils, volunteers, contractors and visitors.
Breaches of this policy may be dealt with under our Staff Code of Conduct

2. Relevant legislation and guidance

This policy refers to, and complies with, the following legislation and guidance:

- Data Protection Act 2018
- The General Data Protection Regulation
- Computer Misuse Act 1990
- Human Rights Act 1998
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Education Act 2011
- Freedom of Information Act 2000
- The Education and Inspections Act 2006
- Keeping Children Safe in Education 2018
- Searching, screening and confiscation: advice for schools

This policy also has regard to the following statutory guidance:

- DfE (2020) ‘Keeping children safe in education’

3. Definitions

- **"ICT facilities":** includes all facilities, systems and services including but not limited to network infrastructure, desktop computers, laptops, tablets, phones, music players or hardware, software, websites, web applications or services, and any device system or service which may become available in the future which is provided as part of the ICT service
- **"Users":** anyone authorised by the school to use the ICT facilities, including governors, staff, pupils, volunteers, contractors and visitors
- **"Personal use":** any use or activity not directly related to the users' employment, study or purpose
- **"Authorised personnel":** employees authorised by the school to perform systems administration and/or monitoring of the ICT facilities
- **"Materials":** files and data created using the ICT facilities including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites, and blogs

4. Unacceptable use

The following is considered unacceptable use of the school's ICT facilities by any member of the school community. Any breach of this policy may result in disciplinary or behaviour proceedings (see section 4.2 below).

Unacceptable use of the school's ICT facilities includes:

- Obtaining, downloading, sending, printing, displaying, distributing or otherwise transmitting or gaining access to materials which are pornographic, obscene, racist, unlawful, abusive, offensive or inappropriate will be regarded as gross misconduct.
- Distributing abusive, discriminatory or defamatory statements will be regarded as gross misconduct and will lead to disciplinary action.
- Using the school's ICT facilities to breach intellectual property rights or copyright
- Breaching the school's policies or procedures
- Activity which defames or disparages the school, or risks bringing the school into disrepute
- Sharing confidential information about the school, its pupils, or other members of the school community
- Connecting any device to the school's ICT network without approval from authorised personnel
- Setting up any software, applications or web services on the school's network without approval by authorised personnel, or creating or using any program, tool or item of software designed to interfere with the functioning of the ICT facilities, accounts or data
- Gaining, or attempting to gain, access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel
- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities
- Causing intentional damage to ICT facilities
- Removing, deleting or disposing of ICT equipment, systems, programs or information without permission by authorised personnel. Only licensed software should be installed.
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation
- Promoting a private business, unless that business is directly related to the school; this includes any buying or selling of goods
- Using websites or mechanisms to bypass the school's filtering mechanisms
- Use of the internet for personal financial gain, gambling, political purposes or advertising

This is not an exhaustive list. The school reserves the right to amend this list at any time. The headteacher will use professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of the school's ICT facilities.

4.1 Exceptions from unacceptable use

Where the use of school ICT facilities is required for a purpose that would otherwise be considered an unacceptable use, exemptions to the policy may be granted at the headteacher's discretion.

4.2 Sanctions

Pupils and staff who engage in any of the unacceptable activity listed above may face disciplinary action in line with the school's policies on behaviour policy and staff code of conduct.

5. Staff (including governors, volunteers, and contractors)

5.1 Access to school ICT facilities and materials

The school's business manager manages access to the school's ICT facilities and materials for school staff. That includes, but is not limited to:

- Computers, tablets and other devices
- Access permissions for certain programmes or files

Staff will be provided with unique log-in/account information and passwords that they must use when accessing the school's ICT facilities.

Staff who have access to files they are not authorised to view or edit, or who need their access permissions updated or changed, should contact the school business manager.

Supply teachers and temporary staff will use the Supply Teacher login which can be obtained from the office. Staff must not let supply teachers use their own unique log in.

5.1.1 Use of phones and email

The school provides each member of staff with an email address.

This email account should be used for work purposes only.

All work-related business should be conducted using the email address the school has provided.

Staff must not share their personal email addresses with parents and pupils, and must not send any work-related materials using their personal email account.

Staff must take care with the content of all email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract.

Email messages are required to be disclosed in legal proceedings or in response to requests from individuals under the Data Protection Act 2018 in the same way as paper documents. Deletion from a user's inbox does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable.

Staff must take extra care when sending sensitive or confidential information by email. Any attachments containing sensitive or confidential information should be encrypted so that the information is only accessible by the intended recipient.

If staff receive an email in error, the sender should be informed and the email deleted. If the email contains sensitive or confidential information, the user must not make use of that information or disclose that information.

If staff send an email in error which contains the personal information of another person, they must inform the business manager immediately and follow our data breach procedure.

Staff must not give their personal phone numbers to parents or pupils. Staff should use phones provided by the school to conduct all work-related business including on school trips. Or, in case of emergency where they need to use their own phone, withhold their number.

School phones must not be used for personal matters.

Staff who are provided with mobile phones as equipment for their role must abide by the same rules for ICT acceptable use as set out in section 4.

Emails sent from school should contain the same professional levels of language and content as applied to letters or other media. You are responsible for the email you send and for any contacts you make that might result in inappropriate emails being received. Posting anonymous messages and forwarding chain letters is forbidden.

5.1.2 – Use of Class Dojo

As a school we use Class Dojo to share messages with parents. All staff must ensure that posts and messages on Class Dojo are written in a professional manner and given the same consideration as any other communication with parents.

When parents contact staff via class Dojo, teachers should not be expected to respond outside of normal working hours.

5.2 Personal use

Staff are permitted to occasionally use school ICT facilities for personal use subject to certain conditions set out below. Personal use of ICT facilities must not be overused or abused. The school business manager may withdraw permission for it at any time or restrict access at their discretion.

Personal use is permitted provided that such use:

- Does not take place during contact time
- Does not constitute 'unacceptable use', as defined in section 4
- Takes place when no pupils are present
- Does not interfere with their jobs, or prevent other staff or pupils from using the facilities for work or educational purposes

Staff may not use the school's ICT facilities to store personal non-work-related information or materials (such as music, videos, or photos).

Staff should be aware that use of the school's ICT facilities for personal use may put personal communications within the scope of the school's ICT monitoring activities (see section 5.5). Where breaches of this policy are found, disciplinary action may be taken.

Staff are also permitted to use their personal devices (such as mobile phones or tablets) in line with the school's safeguarding policy – section 10.

Staff should be aware that personal use of ICT (even when not using school ICT facilities) can impact on their employment by, for instance putting personal details in the public domain, where pupils and parents could see them.

Staff should take care to follow the school's guidelines on social media (see appendix 1) and use of email (see section 5.1.1) to protect themselves online and avoid compromising their professional integrity.

5.2.1 Personal social media accounts

Members of staff should ensure that their use of social media, either for work or personal purposes, is appropriate at all times.

The school has guidelines for staff on appropriate security settings for social media accounts (see appendix 1).

5.3 Remote access

We allow staff to access the school's ICT facilities and materials remotely.

All staff laptops are set up for remote access to the school server on home networks. This is managed by the School Business Manager and ICT support technician.

Staff accessing the school's ICT facilities and materials remotely must abide by the same rules as those accessing the facilities and materials on-site. Staff must be particularly vigilant if they use the school's ICT facilities outside the school and take such precautions as the business manager may require from time to time against importing viruses or compromising system security.

Our ICT facilities contain information which is confidential and/or subject to data protection legislation. Such information must be treated with extreme care and in accordance with our data protection policy.

5.4 School social media accounts

The school has an official Facebook page, managed by the website manager. Staff members who have not been authorised to manage, or post to, the account, must not access, or attempt to access the account.

SOKs also has a private Facebook page which is managed by the SOKs chair. This is a private group only for parents of children at Kingsway and membership is monitored through security questions.

The school has guidelines for what can and cannot be posted on its social media accounts. Those who are authorised to manage the account must ensure they abide by these guidelines at all times.

5.5. Photos

Staff **must** only use school equipment to record, or take photographs of pupils, and only then if the relevant permission has been obtained. Photos must only be stored using school equipment and must not be uploaded to any home devices.

5.6 Monitoring of school network and use of ICT facilities

The school reserves the right to monitor the use of its ICT facilities and network. This includes, but is not limited to, monitoring of:

- Internet sites visited
- Bandwidth usage
- Email accounts
- Telephone calls
- User activity/access logs
- Any other electronic communications

Only authorised ICT staff may inspect, monitor, intercept, assess, record and disclose the above, to the extent permitted by law.

The school monitors ICT use in order to:

- Obtain information related to school business
- Investigate compliance with school policies, procedures and standards
- Ensure effective school and ICT operation
- Conduct training or quality control exercises
- Prevent or detect crime
- Comply with a subject access request, Freedom of Information Act request, or any other legal obligation

6. Pupils

6.1 Access to ICT facilities

Children have access to the following ICT facilities:

Desktop computers in the ICT suite library.

Desktop computers within classrooms.

Laptop computers which are used both in the ICT suite and in classrooms.

Tablets for use in class.

All ICT facilities should only be used in the presence of staff who should always monitor children's use.

6.2 Search and deletion

Under the Education Act 2011, and in line with the Department for Education's guidance on searching, screening and confiscation, the school has the right to search pupils' phones, computers or other devices for pornographic images or any other data or items banned under school rules or legislation.

The school can, and will, delete files and data found on searched devices if we believe the data or file has been, or could be, used to disrupt teaching or break the school's rules.

6.3 Unacceptable use of ICT and the internet outside of school

The school will sanction pupils, in line with the behaviour policy and/or the anti-bullying policy, if a pupil engages in any of the following **at any time** (even if they are not on school premises):

- Using ICT or the internet to breach intellectual property rights or copyright
- Using ICT or the internet to bully or harass someone else, or to promote unlawful discrimination

- Breaching the school's policies or procedures
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate
- Activity which defames or disparages the school, or risks bringing the school into disrepute
- Sharing confidential information about the school, other pupils, or other members of the school community
- Gaining or attempting to gain access to restricted areas of the network, or to any password protected information, without approval from authorised personnel
- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities
- Causing intentional damage to ICT facilities or materials
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation
- Using inappropriate or offensive language

6.4 – E-safety and the curriculum

We believe that the key to developing safe and responsible behaviours online, not only for pupils but everyone within our school community, lies in effective education. We believe we have a duty to help prepare our pupils to safely benefit from the opportunities the internet brings. We are committed to providing children with age appropriate e-safety messages throughout our curriculum in a variety of ways:

- E-safety teaching through both the PINK (People in the Know) curriculum for PSHE and the computing curriculum (Purple Mash resources).
- We will celebrate and promote e-Safety through a planned programme of assemblies and whole-school activities, including promoting Safer Internet Day each year.
- Use of visitors and external resources such as the PCSO to further support online safety messages.
- We will discuss, remind or raise relevant e-Safety messages with pupils routinely wherever suitable opportunities arise during all lessons; including the need to protect personal information, consider the consequences their actions may have on others, the need to check the accuracy and validity of information they use and the need to respect and acknowledge ownership of digital materials.
- All staff will model safe and responsible use of the internet through all areas of the curriculum and provide pupils with guidance on how to safely respond to content categorised under the three main areas of risk: content, contact and conduct (KCSIE 2020).
- Pupils will be taught about the impact of online bullying and know how to seek help if they are affected by any form of online bullying. See Anti-Bullying Policy.
- Pupils will be made aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent or carer, teacher or trusted staff member, or an organisation such as Childline or the CEOP report abuse button.

7. Parents

7.1 Access to ICT facilities and materials

Parents do not have access to the school's ICT facilities as a matter of course.

However, parents working for, or with, the school in an official capacity (for instance, as a volunteer or as a member of SOKs) may be granted an appropriate level of access, or be permitted to use the school's facilities at the headteacher's discretion.

Where parents are granted access in this way, they must abide by this policy as it applies to staff.

7.2 Communicating with or about the school online

We believe it is important to model for pupils, and help them learn, how to communicate respectfully with, and about, others online.

Parents play a vital role in helping model this behaviour for their children, especially when communicating with the school through our website and social media channels.

8. Data security

The school takes steps to protect the security of its computing resources, data and user accounts. However, the school cannot guarantee security. Staff, pupils, parents and others who use the school's ICT facilities should use safe computing practices at all times.

8.1 Passwords

All users of the school's ICT facilities should set strong passwords for their accounts and keep these passwords secure.

Users are responsible for the security of their passwords and accounts, and for setting permissions for accounts and files they control.

Members of staff or pupils who disclose account or password information may face disciplinary action. Parents or volunteers who disclose account or password information may have their access rights revoked.

8.2 Software updates, firewalls, and anti-virus software

All of the school's ICT devices that support software updates, security updates, and anti-virus products will be configured to perform such updates regularly or automatically.

Users must not circumvent or make any attempt to circumvent the administrative, physical and technical safeguards we implement and maintain to protect personal data and the school's ICT facilities.

Any personal devices using the school's network must all be configured in this way.

8.3 Data protection

All personal data must be processed and stored in line with data protection regulations and the school's data protection policy.

8.4 Access to facilities and materials

All users of the school's ICT facilities will have clearly defined access rights to school systems, files and devices.

These access rights are managed by the School Business Manager

Users should not access, or attempt to access, systems, files or devices to which they have not been granted access. If access is provided in error, or if something a user should not have access to is shared with them, they should alert the school business manager immediately.

Users should always log out of systems and lock their equipment when they are not in use to avoid any unauthorised access. Equipment and systems should always be logged out of and closed down completely at the end of each working day.

When users need to leave the room whilst their computer is logged on, the screen should be locked.

8.5 Encryption

The school ensures that its devices and systems have an appropriate level of encryption.

School staff may only use personal devices (including computers and USB drives) to access school data, work remotely, or take personal data (such as pupil information) out of school if they have been specifically authorised to do so by the headteacher.

Use of such personal devices will only be authorised if the devices have appropriate levels of security and encryption, as defined by the ICT manager/SBM.

9. Internet access

The school wireless internet connection is secured and staff and children have access to different drives on the server.

Unfortunately, along with a wealth of useful educational sites on the internet, there are also sites which contain inappropriate materials which it would be unacceptable for children to gain access to.

To ensure that children access the internet within a safe environment our internet service is filtered by the SWgFL. This excludes unacceptable material through filtering lists of inappropriate sites to which access is barred when using the school's line. However, there is a very small risk that inappropriate material may occasionally get through unfiltered. If this happens the the SWgFL should be contacted and the headteacher should be informed.

9.1 Pupils

Internet access is a necessary part of planned lessons. It is an entitlement for pupils based on responsible use. Teachers will ensure that:

- Pupils will be taught how to use a range of age-appropriate online tools in a safe and effective way.

- For Foundation and Key Stage 1, access to the Internet will be by teacher or adult demonstration or suitable skills will be taught / activities provided to ensure that children are only accessing appropriate sites.

- For Years 3 and 4, access to the Internet will be by teacher or adult demonstration. Pupils will access teacher-prepared materials or specific sites deemed safe by staff and searching will only take place using the search engine 'Swiggle.'

- For Years 5 and 6, Internet access will be granted to a whole class as part of the scheme of work, after a suitable introduction to the rules for responsible Internet use. In the normal event, access will be guided by using sites listed in the school Intranet pages and safe search techniques will be taught.

9.2 Parents and visitors

Parents and visitors to the school will not be permitted to use the school's wifi unless specific authorisation is granted by the headteacher.

The headteacher will only grant authorisation if:

- Parents are working with the school in an official capacity (e.g. as a volunteer or as a member of SOKs)
- Visitors need to access the school's wifi in order to fulfil the purpose of their visit (for instance, to access materials stored on personal devices as part of a presentation or lesson plan)

Staff must not give the wifi password to anyone who is not authorised to have it. Doing so could result in disciplinary action.

Tapestry:

Parents of children in EYFS and year 1 have access to their children's learning via Tapestry. Before children's accounts are activated, parents are asked to sign an agreement (see appendix iii)

10. Monitoring and review

The headteacher and the SBM monitor the implementation of this policy, including ensuring that it is updated to reflect the needs and circumstances of the school.

This policy will be reviewed every year.

The governing board is responsible for approving this policy.

11. Related policies

This policy should be read alongside the school's policies on:

- Online safety
- Safeguarding and child protection
- Behaviour
- Staff Code of Conduct
- GDPR
- Anti-bullying.
- RSE

BREACHES OF THE POLICY

- Any breach of this policy may be investigated and may lead to disciplinary action being taken against the staff member/s involved in line with School Disciplinary Policy and Procedure.

- A breach of this policy leading to breaches of confidentiality, or defamation or damage to the reputation of the school or any illegal acts or acts that render the school or the County Council liable to third parties may result in disciplinary action or dismissal.

- Contracted providers of the school must inform the relevant service or County Council officer immediately of any breaches of this policy so that appropriate action can be taken to protect confidential information and limit the damage to the reputation of the service and the County Council. Any action against breaches should be according to contractors' internal disciplinary procedures.

If you are in doubt about any of the above, please seek advice.

Appendix 1: Social Media guidelines for staff:

Social Media
Social Media is used increasingly across society and is recognised as a hugely valuable communication tool. However, the open nature of the internet means that social networking sites can leave professionals (such as teachers and other staff working in education) vulnerable if they fail to observe a few simple precautions. This policy is designed to protect school staff and pupils from potential harm or from becoming victims of radicalisation, extremism and malicious, upsetting or inadvisable contact. (For detailed explanations please see the School Safeguarding Policy)

- Staff members **must not** identify themselves as employees of the school in their personal webspace apart from professional websites such as LinkedIn. This is to prevent information on these sites from being linked with the school and the County Council and to safeguard the privacy of staff members, particularly those involved in providing sensitive frontline services.

- Staff members **must not make contact through any personal ICT or social medium with any pupil**, whether from our school or any other school, unless the pupil* is your own family member OR an existing close family friend. School does not expect staff members to discontinue contact with their own family members or significant family friends via personal social media, however care should be taken not to communicate with friends of the family member who may be school pupils.

- We strongly advise against accepting social media 'friend' invites from parents of pupils. There may exceptions to this e.g. the parent is a family member.

- If staff members need to communicate with parents or pupils for work purposes they can only do so through the official school email, Class Dojo or school phone. Personal email addresses/phone numbers **must not** be shared with pupils or parents.

- Staff members **must decline 'friend requests' from pupils or former pupils (those who have left the school within the last 5 years)** they may receive in their personal social media accounts. Pupils/parents will be informed that this will be the case on induction.

- On leaving school employment, staff members **must not** contact pupils by means of personal social media sites. Similarly, staff members must not contact pupils from their former schools by means of personal social media.

- Any information staff members have access to as part of their employment, including personal information about pupils and their family members, colleagues, County Council staff and other parties and service or County Council corporate information must not be discussed on their personal webspace or social media sites.

- Photographs, videos or any other types of image of pupils and their families or images depicting staff members who can be identified as school staff must not be published on personal webspace or social media sites.

- School or County Council email addresses and other official contact details must not be used for setting up personal social media accounts or to communicate through such media.

- Staff members must not edit open access online encyclopaedias such as *Wikipedia* in a personal capacity at work. This is because the source of the correction will be recorded as the employer's IP address and the intervention will, therefore, appear as if it comes from the employer itself.

- School logos or brands must not be used or published on personal webspace/social media sites (apart from professional websites such as LinkedIn)

- School does not permit personal use of social media or the internet during core contracted work hours. Access to social media sites for personal reasons is not allowed between 9am and 4.15pm (apart from during lunch breaks). Staff members are expected to devote their contracted hours of work to their professional duties.

- **Caution** is advised when inviting work colleagues to be 'friends' on personal social networking sites. Social networking sites blur the line between work and personal lives and it may be difficult to maintain professional relationships or it might be just too embarrassing if too much personal information is known in the work place. Staff **must not** use social media and the internet in any way to attack, insult, abuse or defame pupils, their family members, colleagues, other professionals, other organisations, School or the County Council.

- Staff members **<u>are advised to set the privacy levels of their personal social media sites as strictly as they can</u>** and to opt out of public listings on social networking sites to protect their own privacy. Staff members should keep their passwords confidential, change them often and be careful about what is posted online; it is not safe to reveal home addresses, telephone numbers and other personal information. It is a good idea to use a separate email address just for social networking so that any other contact details are not given away. *(Please see the "Social networking – Guidelines for NASUWT members which sets out minimum recommended privacy settings for Facebook)*

What do to if…

A pupil adds you on social media

- In the first instance, ignore and delete the request. Block the pupil from viewing your profile
- Check your privacy settings again, and consider changing your display name or profile picture
- If the pupil asks you about the friend request in person, tell them that you're not allowed to accept friend requests from pupils and that if they persist, you'll have to notify senior leadership and/or their parents. If the pupil persists, take a screenshot of their request and any accompanying messages
- Notify the senior leadership team or the headteacher about what's happening

A parent adds you on social media

- It is at your discretion whether to respond. Bear in mind that:

  Responding to one parent's friend request or message might set an unwelcome precedent for both you and other teachers at the school

  Pupils may then have indirect access through their parent's account to anything you post, share, comment on or are tagged in

- If you wish to decline the offer or ignore the message, consider drafting a stock response to let the parent know that you're doing so

You're being harassed on social media, or somebody is spreading something offensive about you

- **Do not** retaliate or respond in any way
- Save evidence of any abuse by taking screenshots and recording the time and date it occurred
- Report the material to the relevant social network and ask them to remove it
- If the perpetrator is a current pupil or staff member, our mediation and disciplinary procedures are usually sufficient to deal with online incidents
- If the perpetrator is a parent or other external adult, a senior member of staff should invite them to a meeting to address any reasonable concerns or complaints and/or request they remove the offending comments or material
- If the comments are racist, sexist, of a sexual nature or constitute a hate crime, you or a senior leader should consider contacting the police

Appendix 2: Acceptable use agreement for pupils

THINK BEFORE YOU CLICK!

I will only use the internet when I have permission.

I will immediately tell an adult if I see something I think I shouldn't when using computers or something that makes me feel uncomfortable.

I will only use search engines, websites to and apps which I have been given permission to use.

I will not share any information about myself or others on the internet.

I will not talk or write to other people online without permission.

I will use tablets and ipads responsibly I and will not take photos or video without permission.

I understand that the internet contains information that may be written by anyone and that some information I read may not be true.

I will be careful what I click on to make sure I don't see or download something by mistake.

I will respect others' work and will not change or delete their files.

I will only bring a mobile phone to school if I have been given permission to do so, and I agree not to use it on the school grounds.

Teachers should discuss these with their classes and ask children to sign up to this; it can be simplified for younger children. They should then sign it as a class.

Appendix iii

Kingsway Primary School

Valley Gardens
Kingsway
Gloucester, GL2 2AR

Tel: 01452 881800
Fax: 01452 881796
Email: admin@kingsway.gloucs.sch.uk

Dear Parent/Carer

At Kingsway Primary School, we highly value parents' involvement in their child's education. We are pleased to inform you that we create your child's 'Learning Journey' through an educational software called **Tapestry**. By logging onto the Tapestry app with a secure username and password, you will be able to view your child's observations, photographs and videos throughout their time with us in Reception and through into Year 1.

You will receive an email when a new observation or piece of work is available for you to view. This will enable you to follow your child's progress closely and you can reflect upon each achievement together with your child. You are also able to respond to any of the observations by adding a comment. We will reference your child's learning to the EYFS profile so you will know which area of learning your child is achieving in and the age-band they were working in for that activity. Please note, this is just **one** of the many forms of assessment we use. All of this information is stored on a highly secure server which is monitored closely.

Our main form of communication with you is through the **Class Dojo** app which you can download onto your phone or ipad/tablet (available for both iOS and Android). We will post class stories and photos to inform you about events, day to day exciting happenings and we can also send messages. Your child will be able to create their own character and we can then award 'Dojos' for a variety of achievements which you will receive notifications about.

E-safety is extremely important to us at Kingsway, therefore we ask you to provide us with the following information and to sign the agreement and other information overleaf to show that you understand and will agree with our guidelines.

If you are unable to access an online facility, please let us know so we can arrange time for you to view your child's Tapestry account in school.

We are sure that you will love this new way of viewing your child's achievements as much as we do!

Kind regards,

Miss Price, Miss Sandy and Mrs Chrimes

Agreed guidelines for accessing and using your child's Tapestry and Class Dojo accounts:

As a parent I will…

- **Not** publish any of my child's observations, photographs or videos on any social media site.
- Keep the login details within my trusted family.
- Speak to a member of staff if I experience any difficulties accessing my child's learning journey.

I agree to the following guidelines:

Print name: ______________________________

Name of child: ___________________________

Signature: _______________________________ Date: ___________________

In order for us to set up each account for you, we require the following information. Once the accounts have been created you will receive notification emails enabling you to set up your password and log in.

Parent/Carer name: ____

Preferred email address: ____