TKS E-Safety Policy Part 2 of 2 (AUP and Permissions)

Written by:	MC/TO	Date:	November 2021
Most recently updated by:	RG	Date:	July 2024
Approved by:	APS	Date:	July 2024
Review frequency:	Bi-annual	Date of next review:	July 2026

CONTENTS

1. Introduction

The King’s School is committed to a policy of protecting the rights and privacy of all individuals. To do this we need to collect and use certain types of data to fulfil our commitments to our staff, pupils, regulatory bodies and volunteers. This personal information must be collected and processed appropriately.

The General Data Protection Regulation (GDPR) guideline governs the use of information about people (personal data). Personal data can be held on computer or in a manual paper file, and may include information relating to emails, meetings, booking details, marketing communications, fundraising as well as photographs of individuals and groups.

The King’s School will remain the data controller for the information held. Staff, pupils’ external data processors (e.g. local education authorities) and volunteers will be personally responsible for processing and using personal information in accordance with the General Data Protection Regulation guidelines.

All staff, pupils and volunteers of The King’s School who have access to personal information, will be expected to read and comply with these policies.

2. This Document

This document is in 2 sections.

1. The eSafety Policy (Part 1) - Policy details
2. The eSafety Policy (Part 2) - This document. It is a compilation of the Acceptable Use Agreements and permission forms that require signing by various users.

TKS E-Safety Policy Part 2 of 2 (AUP and Permissions)

Below is a table of the various forms to sign and who should sign which form

TKS E-Safety Policy Part 2 of 2 (AUP and Permissions)

Form	Description	What to do	Process
1. Pupil Acceptable Use Agreement and Form – Secondary Pupils	All secondary school pupils must sign this yearly before being allowed to use TKS IT systems.	**Secondary** All Secondary Pupils, each year sign and return	Pupils complete on first day of Y7; in online pupil form
2. Pupil Acceptable Use Agreement – Primary (Y**1** – Y6)	All school pupils Y1-6 and parents/Carers, before enrolling at TKS	**Non Secondary** Pupil (and parent/carer) sign and return	Online pupil form
3. Acceptable Use Agreement - Early Years Pupils (N1, N2, YR) including Remote learning	Early Years agreement and form (including remote learning)	Parent/Carer Early Years sign and return	
4. Parent / Carer Acceptable Use Agreement (Primary and Secondary)	All parents/Carers	Parent/Carer sign and return	Parents read and agree in online pupil form
5. Acceptable Use Policy and Parent/Carer Permission Form for Remote Learning (Primary Y3-6)	All Y3-Y6 school pupils and parents/carers Registrar keep returned forms in the pupils folder held in Principal's office	Pupil and parent/carer Y3-6 Remote Learning	Parents read and agree in online pupil form
6. Acceptable Use Policy and Parent/Carer Permission Form for Remote Learning (Secondary)	All senior school pupils and parents/carers Registrar keep returned forms in the pupils folder held in Principals office	Secondary Pupil and parent/carer	Parents read and agree in online pupil form
7. Use of Digital / Video Images Permission Form	Video/photo usage standard and permissions form	Parent/Carer and pupil	Parents read and agree in online pupil form
8. Acceptable Use Agreement – Staff and Volunteer	ICT standard to follow	Signed at Induction	
9. School Technical Security Policy (including passwords)	Password standards to adhere to	Signed at Induction	
10. School Personal Data Handling Policy	Data handling standards to adhere to	Signed at Induction	
11. Bring Your Own Device Pupil Contract	An agreement of conditions for Secondary pupils who have been given permission to bring their own device to school to meet their SEND needs.	Signed by pupil and emailed to parents	SENCO approves device; contract is signed; IT check device and connect to network.

3. Pupil Acceptable Use Agreement and Permission Form – Secondary Pupils

Digital technologies have become integral to the lives of children and young people, both within and outside school. These technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning, however they can be misused. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other digital technologies; and,
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

The school will try to ensure that *pupils* will have good access to digital technologies to enhance their learning and will, in return, expect the *pupils* to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users.

For my own personal safety:

- I understand that the school will monitor my use of the systems, devices and digital communications.
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will be aware of "stranger danger", when I am communicating on-line.
- I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc.)
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the school ssystems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission from a member of staff.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not use the school systems or devices for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (e.g. YouTube), unless I have permission of a member of staff to do so.

I will act as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive, inappropriate language and I appreciate that others may have different opinions.

- I will not take or distribute images of anyone without their permission.

I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of The King's School:

- I will only use my own personal devices (mobile phones / USB devices etc.) in school if I have permission. I understand that, if I do use my own devices in The King's School, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.
  - If permission is given, I will virus scan any external storage devices (e.g. USB stick) before copying any data from it to school computers.
    Note. If you do not know how to do this please ask the IT department.
- I understand the risks and will make every effort not to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programs or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person / organisation who sent the email, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programs)
- I will not install or attempt to install or store programs of any type on any school device, nor will I try to alter computer settings.

When using the internet for research or recreation, I recognise that:

- I should ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not try to download copies (including music and videos)
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

I understand that I am responsible for my actions, both in and out of school:

- I understand that The King's School also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may include loss of access to the school network / internet detentions, suspensions, contact with parents and (in the event of illegal activities) involvement of the police.

Please complete the sections on the next page to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school systems and devices.

Permission Form

Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school ICT systems.

I have read and understand the above and agree to follow these guidelines when:

- I use The King's School systems and devices (both in and out of school)
- I use my own devices in The King's School (when allowed) e.g. mobile phones, kindle, gaming devices USB devices, cameras etc.
- I use my own equipment out of the school in a way that is related to me being a member of this school communicating with other members of the school, accessing school email etc.

Name of Student / Pupil

Group / Class

Signed

Date

4. Pupil Acceptable Use Agreement – Primary (Y1 – Y6)

This is how we stay safe when we use electronic devices:

- I will ask a teacher or suitable adult if I want to use the computers or iPads
- I will only use activities that a teacher or suitable adult has told or allowed me to use.
- I will take care of the computer and other equipment
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something
- I will tell a teacher or suitable adult if I see something that upsets me on the screen.
- I know that if I break the rules I might not be allowed to use a computer.

Signed (child):……………………………………………

Signed (parent): …………………………………………..

5. Acceptable Use Agreement Early Years Pupils (N1, N2, YR) including remote learning

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning; however, they can be misused. Children and young people should have an entitlement to *safe* internet access at all times.

This agreement is primarily related to your role as parents/guardians of these pupils in the following possible scenarios:

- supporting your child in remote learning sessions, as requested by SSFU staff (for example, in the event of a lockdown)

- online assemblies and other wider school gatherings online

- parent meetings with staff online

The agreement also covers use of the internet and ICT systems by pupils in school.

This Acceptable Use Agreement is intended to ensure the following:

- Parents and Guardians will be responsible users and stay safe while using the internet and other digital technologies.
- School systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- Parents and carers are aware of the importance of e-safety and are involved in the education and guidance of their children with regard to appropriate on-line behaviour.
- Parents do not use or share personal information and/or digital images of school pupils (taken during school activities) without school's permission.

Should you have any safeguarding concerns arising from your use or your child's use of online platforms in connection with school, please report these in the normal way to the DSL (Designated Safeguarding Lead).

Parents are requested to sign this permission form to indicate their agreement.

Permission Form

Parent/Carer's Name: ……………………………………………………………………………………………………..

Pupil's Name: …….

As the parent / carer of the above pupil(s), I give permission for my son / daughter to have access to the internet and to ICT systems at school.

- I know that my son / daughter has signed or will sign an Acceptable Use Agreement at an appropriate age and has received, or will receive, appropriate e-safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

- I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems at school. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

- I understand that my son's / daughter's activity on the ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the school's data protection and IT policies.

- I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's e-safety.

- I will not use or share personal information and/or digital images of school pupils (taken during school activities) without school's permission.
- I agree to participate in online activity with school from a communal space and not a private bedroom where possible. I will ensure that any background does not show inappropriate images or documentation, and that any persons in view are appropriately dressed.

- My child will be under the supervision of a responsible parent / carer when taking part in online school gatherings or remote learning.

- I will ensure my child's participation in online gatherings or remote learning is respectful and considerate to others.

Signed:

Date:

6. Parent / Carer Acceptable Use Agreement (Primary and Secondary)

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning, however they can be misused. Young people should have an entitlement to *safe* internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other ICT equipment
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that parents and carers are aware of the importance of e-safety and are involved in the education and guidance of young people with regard to their on-line behaviour.
- that the parents do not use or broadcast digital images of school pupils without permission
- the school will try to ensure that pupils will have good access to digital technologies to enhance their learning and will, in return, expect the pupils to agree to be responsible users. A copy of the Pupil Acceptable Use Policy is attached to this permission form, so that parents / carers will be aware of the school expectations of the young people in their care.

  Parents are requested to sign the permission form below to show their support of the school in this important aspect of the school's work.

Permission Form

Parent / Carers Name

Pupil Name

As the parent / carer of the above pupil(s), I give permission for my son / daughter to have access to the internet and to ICT systems at school.

I know that my son / daughter has signed or will sign an Acceptable Use Agreement at an appropriate age and has received, or will receive, appropriate e-safety education to help them understand the importance of safe use of technology and the internet – both in and out of The King's School.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my son's / daughter's activity on the ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's e-safety.

Signed

Date

7. Acceptable Use Policy and Parent Permission Form for Remote Learning (Primary Y3 to Y6)

Introduction

When remote learning is being delivered the existing TKS Acceptable Use Policy and Safeguarding policy that you have previously signed still applies.

This document covers/emphasizes additional guidance related to e-learning sessions. Specifically,

- Remote 1-to-many type gatherings (e.g. virtual classrooms, assemblies etc.) and
- Teacher to pupil (1 to 1) meetings

The 'Prevent Duty' and all other basic safeguarding approaches will always be applied by the school. Please contact the DSL (Designated Safeguarding Lead) at school in the normal way to report any concerns which arise while using online platforms in the event of enforced school buildings closure.

General Online Safety Guidelines

a) Pupils can only use this e-learning platform if approved by the parent/carer.

b) The parent/carer and pupil must sign and return the approval form (below) to their class teacher for the pupil to participate in the eLearning environment.

c) Pupils should ensure the background to any video conferencing is neutral and does not show any inappropriate images or documentation. We recommend pupils participate in MS Teams video calls from a communal area (lounge, kitchen etc.) but we understand this is not necessarily possible due to the need for minimal distractions during learning. Should your child be away from a common area, for example be in their bedroom; please do your best to have open doors and an adult nearby, being appropriately dressed.

d) Pupils should ensure communications in the gatherings are conducted in the same manner they would in a school classroom.

e) Pupils should report any concerns to parents who can then call the school and ask to speak to the safeguarding lead.

f) Parents who choose to host online sessions with children other than their own must ensure they comply with the school's Safeguarding Policy in full. They cannot use the school online learning facility if school staff are not present in the sessions.

g) Pupils should not share their login details

What you need to do now

a) Read this document, and ensure both you and your child, are familiar with the conditions of participating in the remote learning environment in section 1.

b) Pupils - Please sign your section of the form below

c) Parents/Carers - Please sign your section of the form, confirm that the pupil under your care has also signed their section, then return your forms to your year child's teacher by email (copy and paste of this document into email is acceptable but please do not return by post).

Remote Learning Acceptable Use Form

Group/ Class	Pupil Name	Pupil Signature	Name of Parent / carer	Parent/Carer Signature	Date

Contact email addresses to use for eLearning communications

Parent Contact Email address (Preferred)	
Parent Contact Email Address (Alternative)	

8. Acceptable Use Policy and Parent Permission Form for Remote Learning (Secondary)

Introduction

When Home Learning is being delivered due to enforced school site closure the existing school Acceptable Use Policy and Safeguarding policy that you have previously signed still applies.
This document focusses on specific guidelines regarding remote 1-to-many type gatherings (e.g. virtual classrooms, tutoring etc.) and serves as additional guidance beyond that already stated in the policy.
The 'Prevent Duty' and all other basic safeguarding approaches will always be applied by the school. Please contact the DSL (Designated Safeguarding Lead) team at school in the normal way to report any concerns which arise while using online platforms in the event of enforced School buildings closure.

General Online Safety Guidelines

a) Pupils can only use this e-learning platform if approved by the parent/carer.
b) The parent/carer and pupil must sign and return the approval form below for the pupil to participate in the eLearning environment.
c) Pupils should ensure the background to any video conferencing is neutral and does not show any inappropriate images or documentation. We would recommend pupils participate from a communal area (lounge, kitchen etc.) but we understand this is not necessarily possible due to the need for minimal distractions during learning.
d) Pupils should ensure communications in the gatherings are conducted in the same manner they would in a school classroom.
e) Pupils should report any concerns to parents who can then call the school and ask to speak to the DSL team.
f) Parents who choose to host online sessions with children other than their own must ensure they comply with the school's Safeguarding Policy in full. They cannot use the school online learning facility if school staff are not present in the sessions.
g) Pupils should not share their login details

What you need to do now

h) Read this document to ensure you are familiar with the conditions of participating in the remote learning environment.
i) Pupil - Please sign your section of the form below
j) Parent/Carer - Please sign your section of the form, confirm that the pupil under your care has also signed their section, then return (photo of the signed form is sufficient) your forms to your year tutor by email. You cannot participate in the remote learning environment until these have been returned.

Remote Learning Acceptable Use Form

Please complete the sections below to show that you have read, understood and agree to the rules included in the above 'General Online Safety' section. If you do not sign and return this agreement, access will not be granted to this remote learning environment.

I have read and understand the above. I agree to follow these guidelines when I use my own equipment outside of The King's School in a way that is consistent with me being a member of The King's School in the way that I communicate with other members of the school community.

Group/ Class	Pupil Name	Pupil Signature	Name of Parent / carer	Parent/Carer Signature	Date

Contact Email addresses to use for eLearning invitations

Parent Contact Email address (Preferred)			
Parent Contact Email Address (Secondary)			
Pupil Name		Pupil email address for eLearning	
Pupil Name		Pupil email address for eLearning	
Pupil Name		Pupil email address for eLearning	

9. Use of Digital / Video Images Permission Form

The use of digital / video images plays an important part in learning activities. Pupils (with permission) and members of staff may use school digital cameras to record evidence of activities in lessons and out of school. These images may then be used in presentations in subsequent lessons.
Internal School Use. Images may be used to celebrate success through their publication internally, in school, and in newsletters
External use. The school will comply with the Data Protection Act and GDPR and request parents / carers permission before publishing images of members of the school on the school website or other external media. We will also ensure that when images are published that the young people cannot be identified by the use of their names.
Parents and Carers. In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other pupils in the digital / video images.
Parents / carers are requested to sign the permission form below to allow the school to take and use images of their children and for the parents / carers to agree

Digital / Video Images Permission Form

Parent / Carers Name

Student / Pupil Name

As the parent / carer of the above pupil, I agree to the school taking and using digital / video images of my child / children. I understand that the images will only be used to support learning activities or in publicity that reasonably celebrates success and promotes the work of the school.	Yes / No
I agree that if I take digital or video images at, or of, – school events which include images of children, other than my own, I will abide by these guidelines in my use of these images.	Yes / No

Signed

Date

10. Acceptable Use Agreement – Staff and Volunteers

School Policy
As a Christian School we believe God sees and knows everything we do. Our first reason for behaving appropriately with digital technology is from the motivation of wanting to please God with our actions. Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning, however they can be misused. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- Staff and volunteers will be responsible users and stay safe while using the internet and other digital technologies
- That school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of ICT in their everyday work.

The school will try to ensure that staff and volunteers will have good access to ICT to enhance their work, to enhance learning opportunities for pupils' learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement
I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that pupils receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed e-safety in my work with young people.

For my professional and personal safety:

- I understand that The King's School will monitor my use of the ICT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of school ICT systems (e.g. laptops, email etc.) out of school, and to the transfer of personal data (digital or paper based) out of school
- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident that I become aware of, to the appropriate person.

I will be professional in my communications and actions when using The King's School ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.

- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the school website / VLE) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use chat and social networking sites in school in accordance with the school's policies
- I will only communicate with pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school has the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my mobile devices (PDAs / laptops / mobile phones etc.) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- With many methods of secure data transfer, The King's School does not use removable media. Only in exceptional circumstances will removable media be used. This must be provided by the IT department and this needs to be encrypted and/or password protected.

No data is not stored longer than necessary and deleted afterwards in compliance with the Data Retention and Disposal Policy.

We do have several caveats to the policy. These are;

1. This does not apply to camera removable media as it is currently not possible to encrypt camera memory cards. In this situation alternative secure methods must be used. Speak to the IT Support team
2. In the exceptional situations that removable media devices are required (e.g. bulk transfer of video footage) the IT department will provide an appropriate secure solution (e.g. encrypted external drive, secure shared cloud based storage)
3. USB devices used with photocopiers are acceptable (as they are a reduced risk)

IMPORTANT - Any removable media that is introduced into the school network MUST be scanned for viruses before any file copying is done. Ask IT Support on how this simple task is done

- I will not use personal email addresses on the school ICT systems without permission.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the source.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material. Adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others.
- I will not try to use any programs or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programs of any type on a machine, or store programs on a computer, nor will I try to alter computer settings, unless this is allowed in school policies

- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the school policy. Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based Protected and Restricted data must be held in lockable storage.
- I understand that data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of the school:

- I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could result in a warning, a suspension, referral to Governors and (in the event of illegal activities) the involvement of the police.

I have read and understood the above and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff / Volunteer Name

Signed

Date

11. School Technical Security Policy (including passwords)

Introduction

Effective technical security depends not only on technical measures, but also on appropriate policies and procedures and on good user education and training. The school will be responsible for ensuring that the *school infrastructure / network* is as safe and secure as is reasonably possible and that:

- users can only access data to which they have right of access
- no user should be able to access another's personal files (other than that allowed for monitoring purposes within the school's policies).
- access to personal data is securely controlled in line with the school's personal data policy
- there is effective guidance and training for users
- there are regular reviews and audits of the safety and security of school computer systems
- there is oversight from senior leaders and these have impact on policy and practice.

Responsibilities

The management of technical security is the responsibility of ActiveIT and TKS

Technical Security

Policy statements

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people will receive guidance and training and will be effective in carrying out their responsibilities:

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements
- There will be regular reviews and audits of the safety and security of school technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- Appropriate security measures are in place to protect the servers, firewalls, switches, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data.
- Responsibilities for the management of technical security are clearly assigned to appropriate and well trained staff
- All users will have clearly defined access rights to school technical systems.

Password Security

A safe and secure username / password system is essential if the above is to be established and applies to all school technical systems, including networks, devices and email

Policy Statements

- All users will have clearly defined access rights to school technical systems and devices. Details of the access rights available to groups of users will be recorded by the Network Manager (or other person) and will be reviewed, by the senior management team.
- All school networks and systems will be protected by secure passwords that are regularly changed

- The "master / administrator" passwords for the school systems, used by the technical staff must also be available to the Headteacher / Principal or other nominated senior leader and kept in a secure place e.g. school safe.

Staff passwords:

- All staff users will be provided with a username and password by our IT support technician who will keep an up to date record of users and their usernames.
- The password must not include proper names or any other personal information about the user that might be known by others
- The account will be "locked out" following 3 successive incorrect log-on attempts
- Temporary passwords e.g. used with new user accounts or when users have forgotten their passwords, shall be enforced to change immediately upon the next account log-on
- Passwords shall not be displayed on screen, and shall be securely hashed (use of one-way encryption)
- Passwords should be different for different accounts, to ensure that other systems are not put at risk if one is compromised and should be different for systems used inside and outside of school
- Passwords should be changed at least every 120 days
- Passwords should not re-used for 6 months and should be significantly different from the previous four passwords. Users cannot re-use passwords on their log-ins.
- Passwords should be different for different accounts, to ensure that other systems are not put at risk if one is compromised
- Passwords should be different for systems used inside and outside of school

12. School Personal Data Handling Policy

Introduction

Schools and their employees should do everything within their power to ensure the safety and security of any material of a personal or sensitive nature

It is the responsibility of all members of the school community to take care when handling, using or transferring personal data that it cannot be accessed by anyone who does not:

- have permission to access that data, and/or
- need to have access to that data.

Data breaches can have serious effects on individuals and / or institutions concerned, can bring the school into disrepute and may well result in disciplinary action, criminal prosecution and fines imposed by the Information Commissioners Office for the school and the individuals involved. Particularly, all transfer of data is subject to risk of loss or contamination.

Anyone who has access to personal data must know, understand and adhere to this policy, which brings together the legal requirements contained in relevant data protection legislation and relevant regulations and guidance.

Policy Statements

The school will base its data retention and disposal on the school's 'Data Retention and Disposal policy'. Documented separately and can be obtained from the school's Data Protection Lead.

Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.

All personal data will be fairly obtained in accordance with the Privacy Notices (on website and can be obtained from the School's Data Protection Lead) and lawfully processed in accordance with the "Conditions for Processing".

Personal Data

The school and individuals will have access to a wide range of personal information and data. The data may be held in a digital format or on paper records. Personal data is defined as any combination of data items that identifies an individual and provides specific information about them, their families or circumstances. This will include:

- Personal information about members of the school community – including pupils / students, members of staff and parents / carers e.g. names, addresses, contact details, legal guardianship details, health records, disciplinary records
- Curricular / academic data e.g. class lists, pupil / student progress records, reports, references
- Professional records e.g. employment history, taxation and National Insurance records, appraisal records and references
- Any other information that might be disclosed by parents / carers or by other agencies working with families or staff members.
- In addition, personal data has a sub-set known as 'sensitive personal data' or 'special categories of data'. These are data relating to a data subjects:
    - racial or ethnic origin
    - political opinions
    - religious or philosophical beliefs
    - trade union membership
    - genetic data

- biometric data for the purpose of unique identification
- health
- sex life or sexual orientation

Responsibilities
The school's compliance manager will keep up to date with current legislation and guidance and will determine and take responsibility for the school's information risk policy and risk assessment. Everyone in the school has the responsibility of handling protected or sensitive data in a safe and secure manner.
Governors are required to comply fully with this policy in the event that they have access to personal data, when engaged in their role as a Governor.

Registration
SchoolPro is the TKS Data Controller on the Data Protection Register held by the Information Commissioner.

Information to Parents / Carers – the "Privacy Notice"
In order to comply with the fair processing requirements of the DPA, the school will inform parents / carers of all pupils of the data they collect, process and hold on the pupils / students, the purposes for which the data is held and the third parties (e.g. LA, DfE, etc.) to whom it may be passed. This privacy notice will be passed to parents / carers through the parent handbook.

Training & awareness
All staff will receive data handling awareness / data protection training and will be made aware of their responsibilities, as described in this policy through:

- Induction training for new staff
- Staff meetings / briefings / Inset
- Day to day support and guidance

Risk Assessments
Information risk assessments will be carried out by Information Asset Owners and DPO to establish the security measures already in place and whether they are the most appropriate and cost effective. The risk assessment will involve:

- Recognising the risks that are present;
- Judging the level of the risks (both the likelihood and consequences); and
- Prioritising the risks.

Secure Storage of and access to data
The school will ensure that ICT systems are set up so that the existence of protected files is hidden from unauthorised users and that users will be assigned a clearance that will determine which files are accessible to them. Access to protected data will be controlled according to the role of the user. Members of staff will not, as a matter of course, be granted access to the whole management information system.
All users will use strong passwords which must be changed regularly, currently every half-term. User passwords must never be shared.
Personal data may only be accessed on machines that are securely password protected. Any device that can be used to access data must be locked if left (even for very short periods) and set to auto lock if not used for five minutes.

All storage media must be stored in an appropriately secure and safe environment that avoids physical risk, loss or electronic degradation.

Secure transfer of data and access out of school

The school recognises that personal data may be accessed by users out of school, or transferred to the LA or other agencies. In these circumstances:

- Users may not remove or copy sensitive or restricted or protected personal data from the school or authorised premises without permission and unless the media is encrypted/ password protected and is transported securely for storage in a secure location (see earlier section – LA / school policies may forbid such transfer);
- Users must take particular care that computers or removable devices which contain personal data must not be accessed by other users (e.g. family members) when out of school
- When restricted or protected personal data is required by an authorised user from outside the organisation's premises (for example, by a member of staff to work from their home), they should preferably have secure remote access to the management information system or learning platform.
- If secure remote access is not possible, users must only remove or copy personal or sensitive data from the organisation or authorised premises if the storage media, portable or mobile device is encrypted and is transported securely for storage in a secure location.
- Users must protect all portable and mobile devices, including media, used to store and transmit personal information using approved encryption software; and
- Particular care should be taken if data is taken or transferred to another country, particularly outside Europe, and advice should be taken from the local authority (if relevant) in this event. (nb. to carry encrypted material is illegal in some countries)

Disposal of data

All data must be disposed of in adherence with the school Data Retention and Disposal Policy for details.