SOUTH DOWNS
LEARNING TRUST

ACCEPTABLE USE POLICY
(ICT, INTERNET, VIRTUAL LESSONS AND LIVE STREAMING, TELEPHONE AND DATA IN TRANSIT)

RATTON SCHOOL

Date approved	May 2024
Date of next Review	May 2026
Status	Statutory
Lead Author	Jay Chaundy

All our policies support our vision and are based on our core virtues

Compassion – Respect – Creativity – Teamwork – Effort - Responsibility

Developing caring, confident and creative students who achieve

Contents

Introduction

Context

The ICT, internet, Virtual lessons and live streaming, telephone and data in transit acceptable use policy covers the use of ICT systems to support learning both at school and from home, the use of telephones, email and the internet by staff, and the use of online tools provided by South Downs Learning Trust (SDLT). This policy is linked to the staff discipline policy, code of conduct, online safety policy and student behaviour policy.

Core approaches

- No communications device, whether school provided or personally owned, may be used for bullying or harassment of others in any form.
- No applications or services accessed by users may be used to bring the school, or its members, into disrepute.
- No communications devices owned by the school may be taken outside of the UK.
- No communications device, whether school provided or personally owned, may be used to access any form of school related information outside the EU.
- All users have a duty to respect the technical safeguards that are in place. Any attempt to breach technical safeguards, conceal network identities, or gain unauthorised access to systems and services, is unacceptable.
- All users have a duty to protect their passwords and personal network logins, and should log off the network or use screen lock when leaving workstations unattended.
- All users should understand that network activity and online communications are monitored, including any personal and private communications made via the school network.
- All users must take responsibility for reading and upholding the standards laid out in the policy.
- Staff may create and upload pre recorded video content which will have a positive impact on, and aid learning. It is acknowledged that video content will help to engage learners who may struggle with a large amount of written content and provide a connection and sense of ongoing community with teachers during closure.

Policy covers:

Staff	**Students**
Password security Email protocol Data protection Anti-virus and firewall security Safe use of equipment Tablet/laptop devices Remote access Monitoring and logging of internet use Action to be taken upon breach of the policy Telephone Virtual lessons and live streaming	Network etiquette and privacy Security Online ordering systems Email Internet search engines Executable (.exe), music and video files Use of personal devices Saving work Accessing Remote Systems Non-Educational Online Activity Vandalism Virtual lessons and live streaming User Agreements
Data in Transit	
Introduction Purpose Other Relevant Policies and Guidance Scope and who the policy applies to Responsibilities Disciplinary and other sanctions 'Common Sense' Precautions Approved secure transfer mechanisms School email Web Interface Mobile Storage Devices Post Use of personal IT Physical (Paper) records Fax You must not! Reporting data loss Definitions Last Word – Remember	

Staff are asked to sign to show they have read the policy and understood its terms and conditions.

Staff

Password security

Access to all systems and services is controlled by a central computing account and password. Staff are allocated their User ID and initial password as part of their induction with SDLT schools. Continued use of your User Account is conditional on your compliance with this policy. User IDs and passwords are not to be shared or revealed to any other party. Those who use another person's user credentials and those who share such credentials with others will be in breach of this policy. The school enforces a password change every 60 days.

Password complexity is in place for all students, staff and governors/trustees accounts.

Email/File Sharing Protocol

Before sending emails consider:

- Whether email is the correct form of communication.
- The content and level of formality.
- Only copy in people who have an immediate need for the information.
- The length of the email.

Receiving and managing emails

- If they require response, consider carefully the use of the "**reply to all**" button.
- Delete unwanted emails promptly.
- Protect yourself from viruses when emailing from home.

Sensitive Information

- Anyone can read the content along the delivery path of emails. Sensitive information should be sent via a secure transfer system (AVCO, s2s, Voltage or as an encrypted Zip File).
- Child Protection issues should not be reported via email. MyConcern should be used for this.

Before sending sharing files consider:

- Whether email address is correct.
- Link settings are correct – anyone/people in your organisation, people with existing access or specific people.

Your school email should not be used for personal messages or for personal accounts. All school emails will be deleted automatically after two years in line with our retention policy.

Data Protection

SDLT schools hold a variety of sensitive data including personal information about students and staff. If you have been given access to this information, you are reminded of your responsibilities under data protection law (GDPR).

You should only take a copy of data outside the school's systems if absolutely

necessary. This includes putting sensitive data onto mobile devices e.g. tablet devices, laptops, memory sticks, CDs/DVDs or into emails. If you do need to take data outside the school, this should only be with the authorisation of the school's Data Protection Officer and should be signed out and signed in upon return.

There are a variety of methods of remote access to systems available that allow you to work on data in-situ rather than taking it outside the school, and these should always be used in preference to taking data off-site.

ICT Support offers a variety of information to help you keep data secure. If you are uncertain about any aspect of data security, you must contact them for advice.

Anti-virus and firewall security

ICT Support installs all computers with current versions of virus protection and firewall software. Users are not to alter the configuration of this software unless permission has been obtained from ICT Support. This software is installed to prevent an attack from malicious software and to prevent loss of data and corruption of programs/files.

If any user suspects viral infection on their machine, they should inform ICT Support immediately. If a virus is detected it will be disconnected from the network until deemed safe.

Safe use of equipment

The users of ICT equipment should always adhere to the following guidelines:

- Any portable computer must be securely locked away when not in use.
- Portable computer security is your responsibility at all times.
- Do not leave the portable computer unattended in a public place or within the school.
- Staff supervising students using ICT equipment should ensure students take reasonable care of such equipment.

Tablet/laptop devices

Where tablet devices or other mobile devices are allocated to staff, they are the property of SDLT and should be looked after with appropriate care. Staff provided with a tablet/laptop device with a power lead and charger are responsible for ensuring all equipment is in working order.

Staff should:

- remember tablet/laptops devices should be used for educational purposes only;
- keep their tablet/laptop device with them or in a secured (locked) area at all times if not;
- keep the four/six-digit security PIN/password on their tablet devices confidential;
- report loss, theft or damage to ICT Support immediately;
- Information/photos held on the tablet/laptop device are the responsibility of the member of staff and the school will not be held accountable for loss;
- All photos will be wiped at the end of every academic year;

Staff should not:

- modify the settings unless instructed by ICT Support
- apply any permanent marks, decorations or modifications to their tablet devices;
- use tablet device for personal reasons; i.e. Facebook, streaming of non-educational videos personal banking, online shopping;

Unacceptable APPs on school devices

- Facebook/social media/messaging apps;
- Non-Educational Games;
- Pinterest;
- Bank/Building Society;
- Apps of an adult nature (sexual/gambling);
- Online shopping (eBay/amazon);
- Dating

Staff device User Agreement

All staff must sign a user agreement to use the device allocated to them for educational purposes only and abide by the use of device regulations outlined above. Failure to do this, the school may ask for the return of the device and school disciplinary action may ensue. Devices must be periodically handed in for routine maintenance, security updating and screening. This includes a set maintenance period over the summer holidays, to ensure the device is ready for the next academic year. In the case of a suspected theft, the school must be informed at the earliest opportunity.

Remote access

Remote connections are considered direct connections to the school network. As such, generally accessing services remotely, subjects the user to the same conditions, requirements and responsibilities of this policy. All connection attempts are logged.

Monitoring and logging of internet use

Activities regarding network transactions may be monitored, logged and kept for an appropriate amount of time. Logs are taken for reasons of security, diagnostic and account/audit reasons. Logs are available only to authorised systems personnel and kept for no longer than necessary and in line with current data protection guidelines. All internet usage is monitored.

Such records and information are sometimes required - under law - by external agencies and authorities.

Action to be taken upon breach of the policy

The GDPR defines a personal data breach as 'a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal information transmitted, stored or otherwise processed'.

If you believe this may have happened, it is important you notify us so we can investigate by emailing.

DPO@ratton.co.uk

We have 72 hours to inform the ICO (Information Commissioner's Office) if a breach has occurred.

In the event a portable school device is damaged or lost as a result of non-compliance with this policy or as a result of other negligent action, then you may be required to make a full or partial contribution towards any reparation/replacement costs, at the discretion of the academy.

Telephone

There will be occasions when employees need to make short, personal telephone calls on school telephones in order to deal with occasional and urgent personal matters. Where possible, such calls should be made and received outside the employee's normal working hours or when they do not interfere with work requirements.

The use of school telephones for private purposes, which are unreasonably excessive or for school purposes that are defamatory, obscene or otherwise inappropriate, may be treated as gross misconduct under the appropriate disciplinary procedure.

The school reserves the right to audit the destination and length of out-going calls and the source and length of in-coming calls.

Virtual lessons and live streaming

Please refer to our Online Safety policy.

Secondary students must not turn on their video, primary students will use video as it is recognized that at this age it is beneficial to their learning. If they do, please remind them in the first instance. Teachers can use their video function if they choose to do so, it is at their discretion. All talk on the chat must be based on the work.

Teaching from home is different to teaching in the classroom.

- Teachers must find a quiet or private room or area to talk to pupils, parents or carers. Remember to set your status to do not disturb.

- When broadcasting a lesson or making a recording, consider what will be in the background.

- When broadcasting a lesson avoid the use of phrases or content which could be misinterpreted; informal language and images could reinforce with students the ability to have informal discussions.

Set up your equipment

- When setting up meetings remember under 'meeting options' to ensure only you can present when live streaming with students.

- If you have to use your device's mic and speakers, remember to mute your mic unless you are actually speaking.

- For video calls, check your webcam's video is clear. Avoid sitting with your back to the window or you'll become a silhouette. You may wish to sit your laptop on top of a pack of paper or similar to raise the eyeline.

- Think about what is behind you when you set up your camera. If you don't want your colleagues seeing your dirty laundry / collection of Star Wars figures / unusual art work then either move them or consider a different location. Teams also has a "blur video background" option available via the menu button on the video toolbar. We recommend using the SDLT wallpaper.

- Make sure you're dressed appropriately: business casual is fine, but no pyjamas please.
- Close doors to make sure you don't have any unexpected visitors

Joining a meeting

- Before you join the meeting, put your phone on silent, and close any other apps that may send you notifications. Pings and beeps from emails can be annoying. If you have the radio on don't forget to turn this off too.
- Join the meeting a few minutes before the start time to make sure everything is working.
- Remember to turn on your camera / microphone as appropriate. Unless you are leading the meeting you probably want to keep your microphone off until it is your turn to speak.

During the meeting

- If students manage to come in with their video switched on, please ask them to switch it off – you cannot control that yourself from inside the meeting.
- Unlike real life, online meetings have a slight delay, just like interviews on TV news. This may take a moment to get used to.
- Try to avoid talking over or interrupting others. If you need to interrupt please use the chat or hands up.
- If you share your screen remember ensure there are no tabs or documents children should not see.
- Speak a little slower than usual, and try to be as clear and concise as possible.
- Leave a reasonable pause for people to ask questions, people will need a moment to unmute their microphone.
- Only a certain number of videos will show to other users. This means raising your hand or waving may not get the attention of others.
- If you want to ask a question, you can use the chat window to get attention.
- Unmute your microphone when you are speaking, and mute it again when you are finished or if someone else is talking.
- It's best to avoid eating and drinking during meetings unless it's over lunch or dinner.
- Stay seated and present

Technical issues

- Your home broadband probably isn't as fast as the work connection. If you find the connection sluggish, you can turn off incoming video using the menu button on the video toolbar. Students videos will be turned off.

Don't worry

Online meetings are very different than face to face meetings and, for new users, will take some getting used to.

The bigger the meeting the more we should pay attention to etiquette.

Remote Parent & Carer Consultation Evening

Remote consultation evenings are very different than face to face meetings and, for new users, will take some getting used to. They will only take place using EduLink one.

For Data protection and Security -

- Staff will not record consultation appointments using personal equipment under any circumstance.

- Parents/carers are not permitted to record consultation appointments using personal equipment under any circumstance.

- Only members of the Ratton School community will be given access to EduLink One – Parents Evening. Parents Evening will be managed in line with current IT security expectations.

Session Management

EduLink One Parents Evening will record the length, time, date and parent attendance of consultation appointments.

Appropriate privacy and safety settings will be used to manage access and interactions.

This includes:

- Parental access linked directly to their child's details on Sims.
- Parents are unable to send messages to staff through this web-based platform.
- The built in 'waiting room' to ensure privacy

Meeting Expectations

Staff will model professional standards during remote sessions as they would in the normal circumstances of parent consultations.

All participants are expected to behave in line with existing Ratton School policies and expectations. This includes:

- Appropriate language and professional conduct will be used at all times,
- Staff will not take or record images for their own personal use.
- Social distancing to remain in place if sharing consultation with colleagues

When sharing screens and conducting remote consultations, participants are required to:

- wear appropriate dress.
- ensure backgrounds of videos are neutral (blurred if possible).
- ensure that personal information and/or unsuitable personal items are not visible, either on screen or in video backgrounds.

Students (Staff Information)

Students are responsible for reporting any misuse of the network to a staff member. Misuse may come in many forms, but it is commonly viewed as any message(s) sent or received that indicate or suggest pornography, unethical or illegal requests, racism, sexism, inappropriate language, any use which may be likely to cause offence and attempts to disrupt or hack into the computer network.

Network etiquette and privacy

Students are expected to abide by the generally accepted rules of network etiquette. These rules include, but are not limited to, the following:

BE POLITE. Never send or encourage others to send abusive messages. Respect the rights and beliefs of others

USE APPROPRIATE LANGUAGE. Remember that you are a representative of the School on a global public system. Never swear, use vulgarities or any other inappropriate language. Illegal activities of any kind are strictly forbidden.

PRIVACY. Do not reveal any personal information to anyone, especially the home address or personal telephone of yourself or any other students.

PASSWORD. Do not reveal your password to anyone. If you think someone has obtained your password, contact a member of ICT Support immediately.

ELECTRONIC MAIL. Electronic mail (e-mail) is not guaranteed to be private. Messages relating to, or in support of, illegal activities may be reported to appropriate authorities.

REFERENCE WORK. Cite references for any facts that you present. Do not copy other people's work and imply that it is your own (i.e. plagiarism). Plagiarism leads to formal action, up to and including, withdrawal from examination and qualifications.

DISRUPTIONS. Do not use the network in any way that would disrupt use of the services by others.

Security

If students identify a security problem, they must tell a member of staff at once and must never demonstrate the problem to another student. All use of the system must be under their own username and password. They must keep their password to themselves and must not share it with friends. Anyone caught disclosing passwords will have their access denied and may be subject to disciplinary action. Any user identified as a security risk may be denied access to the system and be subject to disciplinary action.

Online ordering systems

Students must not use the Internet for ordering goods or services regardless of their nature. Also, students must not subscribe to any newsletter, catalogue or other form of correspondence via the Internet, regardless of its nature in school or using school electronic mail.

Email

Electronic mail (email) is provided by SDLT schools. The sending or receiving of any email, which contains any inappropriate material, is strictly forbidden. This material includes, but is not limited to, pornography, unethical or illegal requests, racism, sexism, inappropriate language, any use that may be likely to cause offence. Disciplinary action will be taken in all cases. It is also forbidden to send large volume emails (spamming).

Internet search engines

Students are required to use Internet search engines responsibly. If students are found to be searching for material unsuitable and in breach of this policy, they will face disciplinary action.

Students must not remove safety filters from Internet Search engines in order to access unsuitable material. This includes but is not limited to the removal of the Safe Search feature.

Executable (.exe), music and video files

Students must not introduce executable files (e.g. '.exe, .cmd, .bat, .bin') to the network, as these can is some cases contain harmful viruses. This includes but is not limited to copying such files onto shared network drives and running them from a memory stick.

Students must not introduce music and video files (e.g. '.mp3, .mp4, .mpeg, .wav, .avi'). These files in many cases are copyrighted and the copying onto shared network drives may breach their copyright.

Students must not download executable, music and video files when using the Trust's Internet provision.

Saving work

Students must not use external media (e.g. USB memory and external hard disks) as their main storage as it is not possible to recover lost or corrupted files. Students are advised to save all files to schools cloud storage where it is routinely backed up and easily accessed both onsite and remotely. Students are advised to regularly save amendments to their files to limit data loss if their service is interrupted.

Accessing Remote Systems

Students are only allowed to access remote systems authorised by SDLT.

Non-Educational Online Activity

Students are not allowed to access non-educational games, media or chat services available online.

Vandalism

Vandalism is defined as any malicious attempt to harm or destroy any equipment or data of another user or of any other networks that are connected to the system. This includes, but is not limited to, the uploading or creation of computer viruses, the willful damage of computer hardware, whether connected to the network or not, the deletion of data from its place of storage.

Virtual lessons and live streaming

Students must not turn on their video. If they do, please remind them in the first instance. The support person can also deal with this so that the presenter can get on with the lesson. Teachers can use their video function if they choose to do so, it is at their discretion. All talk on the chat must be based on the work.

Below is our script for student expectations script for 'live lesson'

Welcome to our _____virtual lesson.

Before we start there are some rules we will all need to follow for you to get the most out of this session.

Firstly, please mute your mic now, this is so that we do not interrupt each other. Do not share your video this will help you not to be distracted.

I will be here using the video/audio function but will share my screen when I need to.

You can enable the chat feature and if you have questions/technical difficulties, where another member of staff will try to support you. This also means that I do not have to stop and read them at the same time as I want you to get the most out of this session.

We will be using the chat feature to communicate with me so please open that alongside your screen. Give me a thumbs up when you are ready.

The teaching session itself will last between 15-20 minutes where I will be actively teaching you how to.....

Please pay attention and follow my screen**.**

User Agreement

Ocklynge Junior School

Pupil Agreement

This Acceptable Use Policy Agreement is intended to ensure:

- that pupils at Ocklynge School will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.

I understand that I must use school devices and systems in a responsible way and that this agreement will keep me safe when I am online at home and at school.

For my own personal safety:

- I know that I will be able to use the internet in Ocklynge School for many different activities and to keep myself and others safe I must use it responsibly.
- I will not share my password with anyone, and I will log off when I have finished using the computer or device.
- I will protect myself by not telling anyone I meet online any of my personal information. This includes my address, my telephone number, my school name.
- I will not send a picture of myself without permission from a teacher or other adult.
- I will not arrange to meet anyone I have met online alone in person without talking to a trusted adult.
- I will tell a teacher or other adult if someone online makes me feel uncomfortable or worried when I am online using games or other websites or apps.

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

- I know that posting anonymous messages or pretending to be someone else is not allowed.
- I know that information on the internet may not be reliable and it sometimes needs checking so I will not download any material from the internet unless I have permission.
- I know that memory sticks/CDs from outside of the school may carry viruses so I will always give them to my teacher so they can be checked before opening them.
- I know that I am not allowed on personal email, social networking sites or instant messaging in Ocklynge School.
- I know that all Ocklynge School devices/computers and systems are monitored, including when I am using them at home.

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

- I will be polite and sensible when I message people online
- I will not be rude or hurt someone's feelings online.
- I will not look for bad language, inappropriate images or violent or unsuitable games, and if I accidently come across any of these I will report it to a teacher or adult in Ocklynge School, or a parent/carer at home.
- If I get unkind, rude, or bullying emails or messages, I will report them to a teacher/adult. I will not delete them, I will show them to the adult.

When working from home (remote learning):

These expectations are in place to help keep me safe when I am learning at home using Microsoft Teams.

- When taking part in a live lesson I understand that I must take part from somewhere appropriate at home (not in my bedroom) with limited distractions and I must wear appropriate clothing;
- I understand that my teachers may mute my microphone and I should wait for them to unmute it rather than unmuting it myself;
- I understand that I should only communicate with my teacher through pre-arranged live lessons or using school email;
- I will not record teacher audio or video presentations, nor will I take screenshots or photos of teachers or other pupils;
- I will not share or distribute any of the teacher presentations and online teaching resources;
- I will not change or edit of any of the teaching resources made available except for their own personal use;
- I will not take, use, share, publish or distribute images of others without their permission;
- I will not share any access links to these remote learning sessions with others;
- I understand that I must behave online as I would in a classroom;
- I will only use the chat feature for work related discussions;
- I have read and talked about these rules with my parents/carers;

- I understand that if I do not follow this agreement, I may not be allowed to use the internet at Ocklynge School.
- I have read and talked about these rules with my parents/carers.

Child's Name…… Child's Signature ……

Class…… Date……

Parent's Name…….....

Parent's Signature…….. Date…….

Ratton School

I understand that the Ratton School Acceptable Use Policy Agreement will help keep me safe online at home and at school.

The Agreement

This Acceptable Use Agreement is intended to ensure:

- that all pupils at Ratton School will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.

- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems at risk. 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.

For my own personal safety:

- I understand that Ratton 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 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)
- In the unlikely event that I have arranged to meet people off-line that I have communicated with on-line, I will do so in a public place and take an adult with me. (Ratton School does not recommend any pupil arranging to meet people in this way unless as part of an educational visit with an authorised member of staff e.g. Digital Leaders Scheme)

- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it online.
- I understand that Ratton School internet filter is there to protect me, and I will not try to bypass it.
- I will make sure that my internet use is safe and legal, and I am aware that online actions have offline consequences.
- I know I must always check my privacy settings are safe and private.

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

- I understand that Ratton School and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission.
- 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 Ratton School systems or devices for on-line gaming, internet shopping, file sharing, or video broadcasting (eg YouTube), unless I have permission of a member of staff to do so.

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

- I will not access or change other people files, accounts, or information.
- 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 or inappropriate language and I appreciate that others may have different opinions.
- I know that bullying in any form (on and offline) is not tolerated and I know that technology should not be used for harassment.
- I will not take or distribute images of anyone without their permission.
- I will write emails and online messages carefully and politely as I know they could be forwarded or seen by someone I did not intend.
- I understand that it may be a criminal offence or breach of Ratton School policy to download or share inappropriate pictures, videos, or other material online. I also understand that it is against the law to take, save or send indecent images of anyone under the age of 18.
- I will always think before I post, I know that text, photos or videos can become public and impossible to delete.

I understand that Ratton School has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school.

- I will not use my own personal devices (mobile phones / USB devices etc) in school.

- I understand the risks and will not try 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 programmes 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 programmes)
- I will not install or attempt to install or store programmes 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 Ratton 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 in line with the school's behaviour policy. 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.

Remote Learning

These expectations are in place to help keep me safe when I am learning at home using Microsoft Teams.

- When taking part in a live lesson I understand that I must take part in lessons from somewhere appropriate at home (not in my bedroom) with limited distractions and I must wear appropriate clothing;
- I will ensure backgrounds of videos are neutral and personal information/content is not visible;

- I will attend lessons in a shared/communal space or room with an open door and/or where possible when I can be supervised by a parent/carer or another appropriate adult.
- I understand that my teachers may mute my microphone and I should wait for them to unmute it rather than unmuting it myself;
- I understand that I should communicate with my teacher through pre-arranged live lessons or using school email;
- I will not record teacher audio or video presentations, nor will I take screenshots or photos of teachers or other pupils;
- I will not share or distribute any of the teacher presentations and online teaching resources;
- I will not edit of any of the teaching resources made available except for my own personal use;
- I will not take, use, share, publish or distribute images of others without their permission;
- I will not share any access links to these remote learning sessions with others;
- If I am concerned about anything that takes place during remote learning, I will inform a suitable adult;
- I understand that I must behave online as I would in a classroom.
- I understand that inappropriate online behaviour or concerns about my safety during remote learning will be taken seriously. This could include not being able to access these lessons, parents/carers being informed or contact with the police if a criminal offence has been committed;
- I will only use the chat feature for work related discussion
- I have read and talked about these rules with my parents/carers.

KS 3/4/5 Pupil Acceptable Use Agreement Form

This form relates to the Pupil Acceptable Use Agreement, to which it is attached.

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 systems.

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

- I use the Ratton School systems and devices (both in and out of school)
- I use my own equipment out of the school in a way that is related to me being a member of this school e.g. communicating with other members of the school, accessing school email, VLE, website etc.

Child's Name…… Child's Signature ……

Class…… Date……

Parent's Name……

Parent's Signature…….. Date……

Acceptable Use of Technology for Parents/Carers

- I have read - and discussed with my child the pupil Acceptable Use of Technology Agreement Policy (AUP) for South Downs Learning Trust and understand that this AUP will help keep my child safe online;
- I understand that the AUP applies to my child's use of South Downs Learning Trust devices and systems on site and at home, and personal use where there are safeguarding and/or behaviour concerns;
- I am aware that the use of South Downs Learning Trust devices and systems may be monitored for safety and security reason to keep my child safe. This monitoring will take place in accordance with data protection, privacy, and human rights legislation
- I understand that my child needs a safe and appropriate place to access remote learning if South Downs Learning Trust is closed in response to Covid-19 or if my child needs to self-isolate at home. I will ensure my child's access to remote learning is appropriately supervised. When accessing video learning, I will ensure they are in an appropriate location (e.g. not in a bedroom) and that they are suitably dressed
- I give permission for my child/ren to access Microsoft Teams.
- I give permission for my child to participate in live lessons with their form teacher and subject teachers;
- I understand that I will be asked for permission by the subject teacher (via email) if my child needs a 1:1 live lesson (e.g. for Learning Support, EAL etc.);
- I understand that any 1:1 live lessons will be recorded and saved on the South Downs Learning Trust server and kept in accordance with data protection;
- I give permission for my child to submit work and upload work related videos to their teacher;
- I understand that South Downs Learning Trust will take every reasonable precaution, including implementing appropriate monitoring and filtering systems, to ensure my child is safe when they use school devices and systems. I understand that South Downs Learning Trust cannot ultimately be held responsible for the nature and content of materials accessed on the internet or if my child is using mobile technologies
- I give permission for my child's work to be used on South Downs Learning Trust Social Media Account;
- I am aware of the importance of safe online behaviour and will not deliberately upload or add any images, video, sounds or text that could upset, threaten the safety of or offend any member of the South Downs Learning Trust community.
- I understand that South Downs Learning Trust will contact me if they have concerns about any possible breaches of the AUP or have any concerns about my child's safety.
- I will inform South Downs Learning Trust or other relevant organisations if I have concerns over my child's or other members of the school communities' safety online.
- I understand that if my child fails to comply with this Acceptable Use Policy Agreement, they may be subject to disciplinary action in line with the school's behaviour policy. 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.

- I know that my child will receive online safety education to help them understand the importance of safe use of technology and the internet – both in and out of South Downs Learning Trust.
- I will support the South Downs Learning Trust online safety approaches and will discuss this agreement and the pupil agreement with my child. I will use appropriate parental controls and will encourage my child to adopt safe use of the internet and other technology at home, as appropriate to their age and understanding.
- I understand that I must have returned this Consent for Remote Learning Form before my child can take part in any Remote Learning.

Child's Name……. Class……

Parents Name…….....

Parents Signature…….. Date…….

Staff Remote Learning AUP

This Remote Learning Acceptable Use Agreement Policy is intended to ensure:

- that staff and volunteers at South Downs Learning Trust will be responsible users and stay safe while using the internet and other communications technologies whilst remotely teaching pupils who are not in school.
- that South Downs Learning Trust users are protected from accidental or deliberate misuse that could put users at risk.
- that staff are protected from potential risk in their use of technology in their everyday work.

South Downs Learning Trust will try to ensure that staff and volunteers have good access to digital technology and training 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.

I understand that I must use South Downs Learning Trust systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that pupils receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

- I will be aware of and understand my responsibilities when delivering remote lessons.
- I understand that communication with children both in the “real” world and through web interactions should take place within explicit professional boundaries.
- I will be aware of the following policies and procedures:

Safeguarding and Child Protection Policy
Behaviour policy
Staff Code of Conduct
Social Media Policy
Policy for the Prevention of Bullying

- I will not use any personal accounts to communicate with pupils and/or parents/carers
- I will not seek to communicate/make contact or respond to contact with pupils outside of the purposes of my work or outside of school hours;
- I will use work provided equipment where possible
- I am aware that online bullying is a safeguarding issue and that any incidents of this must be reported to the DSL as per South Downs Learning Trust Safeguarding procedures.
- I will report any suspected misuse or problem to the Online Safety Coordinator (DSL) or Network Manager for investigation / action / sanction
- If I am a Form /Class teacher, I will ensure all my pupils have understood and returned the Pupil Remote Learning Home Agreement;
- If I am a Form /Class teacher, I will provide remote pastoral care for my class;
- I will continue to look out for signs that a child may be at risk whilst teaching remotely;
- I understand that it is best practice that staff will guide pupils to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches., e.g. Google Images.
- I will be mindful of the added pressure that remote learning can add to any household and, in particular, in a household with more vulnerable children,
- If I am a SEN or EAL teacher, I will provide assistance to teachers who require help to differentiate and will ensure contact with pupils and their parents who are likely to require further assistance.
- If I am a Form /Class teacher, I will ensure I have regular contact with my class;
- I will make contact with pupils only via South Downs Learning Trust provided email accounts or logins.
- When recording videos and for live lessons I understand that I must wear appropriate clothing
- I understand that for live lessons at least 2 members of staff should be present and where this is not possible the leadership team approval will be sought.
- I understand that live lessons should be recorded and backed up on Teams Streams, so that if any issues were to arise, the video can be reviewed and I understand that these recordings will be kept in accordance with data protection.

- I understand that any 1-1 live lessons need to be pre-arranged, with written parental consent given and that two adults need to be present. Where 1-1 sessions may be necessary these sessions must be recorded and saved to the school server where this can be reviewed at any time.
- I will not record lessons or meetings using personal equipment.
- I understand that any computers used for such recordings or live lessons should be in appropriate areas, for example, not in bedrooms; and where possible be against a neutral background.
- I understand that live lessons should be recorded and backed up on Teams Streams, so that if any issues were to arise, the video can be reviewed and I understand that these recordings will be kept in accordance with data protection.
- I understand that all my language must be professional and appropriate, including if any of my family members are in the background;
- I will not give out my personal details;
- I will not take images of pupils for my own personal use;
- I will not display or distribute images of pupils unless they have parental consent to do so (and, where appropriate, consent from the child)
- At the beginning of each session I will remind pupils of behaviour expectations and reporting mechanisms at the start of the session, including the use of microphones and chat features.
- I will remind pupils to report concerns during remote and/or live streamed sessions:
- If inappropriate language or behaviour takes place, pupils involved will be removed by staff, and concerns will be reported to DSL.
- Inappropriate online behaviour will be responded to in line with existing policies such as acceptable use of technology, allegations against staff, anti-bullying and behaviour.
- I will report any safeguarding concerns will be reported to South Downs Learning Trust School Designated Safeguarding Lead, in line with our child protection policy.

I have read and understood the Remote Learning Acceptable Use Policy (AUP) for staff.

Name: ……

Date…….

Data in Transit

Key points:

- All employees and governors are personally responsible for taking reasonable and appropriate precautions to ensure that all sensitive and confidential data is protected.
- All sensitive and confidential electronic data being taken outside of its normally secure location must be encrypted.

- Data loss must be reported immediately to the headteacher
- Disciplinary action could be taken where employees do not follow the guidance set out in this Policy.

Introduction

Sensitive and confidential data must be treated with appropriate security by all who handle them. 'Appropriate' is not defined in terms of hard and fast rules, but is meant to be a degree of precaution and security proportionate to the potential impact of accidental disclosure. It is not possible to set out precautions and actions to cope with all circumstances and conditions, therefore staff handling sensitive and confidential data MUST assume personal responsibility and make considered judgements in terms of how they handle data and if in any doubt, seek support from their DPO.

Overall impact is determined by the degree of sensitivity of the data and the quantity involved, but we must remember that a single record about an individual can have a potentially massive impact on that individual if accidentally disclosed to others.

Consider: If you were working on very sensitive and private information about yourself, carrying it with you or sending it to someone - what would you do to protect it?

Purpose

This document is intended to prevent unauthorised disclosure of information by laying down clear standards of practice to maintain good security when using, taking or sending sensitive or confidential data outside of their normally secure location.

The need for this is driven by our duty to protect the information of individuals and the school. This duty arises from legislation relating to information security, the most notable of which is as follows;

- General Data Protection Regulation
- Data Protection Act 2018
- Computer Misuse Act 1990
- Freedom of Information Act 2000
- Human Rights Act 2000

A list of definitions is included at the end of this policy document to explain some of the terms used.

Other Relevant Policies and Guidance

This policy does not stand alone, but should be read and acted upon in conjunction with the schools:

- Data Protection and Information Security Policy
- Acceptable Use Agreements
- Code of Conduct
- Others as necessary

Scope and who the policy applies to

The scope covers all circumstances where sensitive or confidential data are taken outside of their normally secure location. This includes data in all formats – non-electronic (paper) and electronic (e.g. on PCs, tablets, laptops and removable storage media – e.g. USB memory sticks).

Whilst the Policy refers to employees and governors, it also applies to temporary staff, volunteers, secondees, work experience candidates, and all staff of service delivery partners and other agencies that process our data.

Responsibilities

The school maintains appropriate security and privacy of data that it uses to perform its functions and it will ensure that appropriate tools, training and guidance are available to staff and members i.e.:

- Secure network for storing and using electronic data
- Secure work locations for storing and using hard-copy data
- Encryption tools for transmission of data outside secure locations

School staff and governors will act in accordance with the following standards and guidance to ensure security and privacy of sensitive and confidential data outside of their normally secure location.

Organisations that use our data to help us deliver a service will have to confirm they comply with these or equivalent standards.

Disciplinary and other sanctions

The school considers this policy to be extremely important.

Where school employees or service delivery partners have acted in accordance with this standard, but a breach occurs through the action of others, they will be deemed to have acted reasonably.

However, if school employees are found to be in breach of the policy and its guidance then they may be subject to disciplinary procedures up to and including dismissal.

'Common Sense' Precautions

There are some 'common sense' precautions that you can take before sending or taking sensitive or confidential data outside of their normally secure location, these are:

- Check that you are not sending/taking more detail than is necessary i.e. will the information still meet the need if you remove the sensitive material or aggregate the data? (GDPR Principle: Data Minimisation)
- Check that the data you are sending/taking are correct and appropriate. (GDPR Principle: Data Accuracy)
- Check that you are sending the data to the correct person/address.
- Check how you intend to keep it secure. (GDPR Principle: Integrity and confidentiality)

The following data transfer methods are ranked in order of security and it is your responsibility to ensure that you use a method and degree of security appropriate to the sensitivity, quantity and potential impact of loss of the data being handled.

Approved secure transfer mechanisms

These are secure transfer mechanisms in use and approved as secure for the purpose. Examples of this are:

- Secure Email
- AVCO AnyComms (software that allows secure transfer of documents)
- School to School (S2S)
- Public Services Network (PSN formally GCSX)
- N3 (The NHS network) including NHS Mail

(This list is not exhaustive and other secure mechanisms will be added), if in doubt ask your Senior ICT Technician or DPO.

School email

Emailing information between internal school mailboxes is secure. However following best practice you should always link or reference information rather than attaching a copy where possible.

If you are sending sensitive or confidential data by email to an external address (other than a secure address) you must:

- Send them as an encrypted email using the designated encryption solution. This may be Voltage Secure Mail but you should check with your IT technician
- If designated encryption solution is not available the document must be encrypted with a password.
- Make sure the recipient is correct, known and trustworthy

Web Interface

If you are transferring sensitive or confidential data through a web portal you must:

- Ensure that there is robust access control in place (i.e. unique username/password)
- Ensure that only the people who need the data can see them
- Ensure that the data are encrypted (https connection)

Mobile Storage Devices

If you are taking data with you on a mobile storage device, such as a tablet PC, laptop, digital camera, smart phone or a USB memory stick you must:

- Make sure that there is no other more secure option available to you
- Only use a school approved device
- Take only as much as necessary, for as long as necessary and transfer them back to their normally secure location as soon as possible
- Keep the decryption PIN, password or token securely and separately from the device/data
- Do not take school equipment outside of the UK without approval from ICT

Take all reasonable precautions to keep the device and data safe and secure e.g.:

- Keep it with you whenever possible; lock it away securely when you can't
- Never leave it in plain sight in public places
- Never let others use your access or device
- Delete the data from the device as soon as possible
- Report loss/theft immediately

Post

The postal service is considered reasonably secure for small amounts or low impact data (i.e. records pertaining to an individual, but NOT including very sensitive personal data). Please refer to any specific school guidance on use of the postal service. As a minimum, there are precautions that you must take to prevent loss:

- Make sure that the recipient and destination address is correct, accurate and up-to-date
- Clearly mark the envelope/parcel with a return address in case of incorrect delivery

- Do not send the only copy of the data if it is practical to make and retain a duplicate. You must assess the impact of loss of the original and make a copy if that impact is unacceptable
- If you use a courier they must be known and trusted
- Consider using recorded/registered post when sending sensitive information
- Make sure it is traceable (i.e. confirmation of receipt)
- Physical records must be sent in a suitable container i.e. robust and secure enough to prevent accidental loss and/or tampering

Use of personal IT

If you are working at home on your own equipment or using a personal online service you must:

- Use a device that has up to date internet security protection in place
- Not transfer sensitive or confidential data to your home PC, laptop or personal online service (e.g. Gmail account, Dropbox etc.)
- Only have as much sensitive or confidential information open as necessary and only for as long as necessary - do not save the data on your device
- Always save the data back to their normally secure location when you have finished
- You must not leave the device unattended for any period of time such that others can access any sensitive data; always lock the device or log out when you are not using it
- Not connect your device to an insecure or unknown network when accessing sensitive or confidential information.

Physical (Paper) records

If you are taking sensitive or confidential information with you in non- electronic (paper) format you must:

- Make sure that there is no other option available to you
- Never take the only copy with you if it is practical to make and retain a duplicate. You must assess the impact of loss of the original and make a copy if that impact is unacceptable (where copies are made, ensure these are securely destroyed as soon as possible following their use).
- Take only as much as necessary and only for as long as necessary
- Transfer it back to its normally secure location as soon as reasonably possible

Take all reasonable precautions to keep the records safe and secure e.g.:

- Keep them with you whenever possible; lock them away securely when you can't
- Use a suitable container that prevents accidental loss and/or viewing by others
- Never leave them in plain sight in public places
- Report loss/theft immediately

Fax

Sending sensitive or confidential information by fax is a last resort and should only be used if the need is urgent and there is no alternative available and you must:

- Use a Fax to E-Mail solution where available

- Make sure the receiving fax machine is in a secure environment
- Make sure the recipient is there to receive it at the time of arrival and that they are known and trusted
- Make sure it is traceable (e.g. confirmation of receipt)

You must not!

There are some data handling activities which are prohibited:

- Never share your network password with anyone and use a different password when encrypting files.
- Sending sensitive or confidential information in unencrypted electronic form without taking appropriate precautions as set out in this policy and guidance.
- Storing sensitive or confidential data on any personal or non-school equipment or in unencrypted form.
- Sending sensitive or confidential information as unsecured physical records.
- Working on sensitive or confidential data on a public device (for example in a library or cafe).
- Working on sensitive or confidential data on a device with an unencrypted wireless (WiFi) connection, i.e. ensure your home wireless network has encryption and use it.
- Leaving sensitive or confidential physical records in plain view of others (i.e. unattended in your office, on the back seat of your car, in a public place, on your kitchen table or even with you, but where they can be overlooked by others).
- Leaving any device holding sensitive or confidential information unattended in a non-secure environment.
- Leaving any device holding sensitive or confidential information in a vehicle overnight

Reporting data loss

Staff should report a loss of sensitive and/or confidential data to the headteacher and complete a data breach incident report form. See the Data Breach Procedure for more information and details of the reporting process.

Definitions

Sensitive and confidential data

The following list is not exhaustive and contains examples of sensitive and confidential data:

- Any data that is marked Official Sensitive/Protect/Restricted (see Appendix 1 Glossary)
- Any data covered by the Data Protection Act - i.e. all data that relates to a living individual.
- Any data classified as Commercial in Confidence - e.g. data that relates to commercial proposals or current negotiations.
- Any data relating to security information, investigations and proceedings, information provided in confidence etc.
- An easy sense check on whether data is sensitive or confidential is to ask:
    - Are the data covered by the Data Protection Act 2018?

- Could release of the information cause problems or damage to individuals, the public, the school, or, a partner organisation? This could be personal, financial, reputation or legal damage.
- Could release prejudice the outcome of negotiations or investigations?

If in doubt, ask your headteacher and err on the side of caution - treat them as sensitive and confidential - do not assume that they are not.

Normally Secure Location
For the purposes of this policy standard 'normally secure location' is defined as:

- A secure network/storage facility with:
  - Access controls such as individual login accounts
  - Backup and recovery facilities
  - No public access
  - Anti-virus and firewall protection
  - Examples are:
    - The school network
    - Schools administrative networks
- Secure buildings or parts of buildings with:
  - Physical access controls - swipe cards, keys etc.
  - No public access
  - Lockable storage facilities
  - Other protection systems e.g.: alarms, CCTV, time locks etc. Examples are:
    - Schools administrative areas (excluding public access areas)

Last Word – Remember:

If you were working on very sensitive and private information about yourself, carrying it with you or sending it to someone what would you do to protect it?

Appendix 1 – Glossary

Personal Data

Personal data is anything that relates to a living individual in which the individual can be identified directly from the information from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller.

Special Category Personal Data

Defined as being any personal data relating to racial or ethnic origin, political opinions, religious or similar beliefs, membership of a trade union, physical or mental health or condition, sexual life, the commission or alleged commission of any offence, any proceedings for any offence committed or alleged to have been committed, the disposal of such proceedings or the sentence of any court in such proceedings.