THE NORTON
KNATCHBULL
SCHOOL

Acceptable ICT use
&
E-Safety Policy

Reviewed by	Matt Gowen, Kevin Robin updated by Tom Sparrow July 2024
Equality Impact Assessment*	Kevin Robin & Matt Gowen
Approved by Finance & General Purposes Committee	26th January 2024
Mobile phone policy reviewed and approved by FGB	16th July 2024
Next Date of Review	Summer 2025
Publication	School Website New starter pack

**The purpose of an Equality Impact Assessment (EIA) is to ensure that policies, functions, plans or decisions do not create unnecessary barriers for people protected under the Equality Act 2010. Where negative impacts are identified these should be eliminated or minimised, and opportunities for positive impact should be maximised.*

1. Rationale : About this acceptable ICT use and E-Safety policy

E-Safety is an essential part of the policy framework of the school for safeguarding, and encompasses elements of behaviour, anti-bullying, PSHCE and other policies.

The policy outlines what the school considers as acceptable use of ICT by its students and its employees in the context of work.

Responsibility for reviewing and updating this policy lies with the E-Learning Co-ordinator together with the Network Manager, Designated Safeguarding Lead and member of the SLT responsible for e-learning. However, the policy has been drawn up in consultation with staff, governors and students, and will continue to evolve as technology and the internet develops.

2. Use of the internet in lessons

Learning the skills in appropriate use of the internet is a vital part of the statutory curriculum, and a vital tool for learning. It is part of everyday life in education, business and social interaction. The school has a duty to provide quality, controlled access to the internet.

Internet use within school :

- should ensure students develop the ability to review and interpret internet content to enhance their learning and produce high quality work ;
- should build on and inform their internet use outside school ;
- is an entitlement to students who show a responsible and mature approach to its use ;
- provides clear, proven educational benefits including

  access to world-wide educational resources including museums and galleries ;

  inclusion in the National Education Network which connects all UK Schools;

  provision of cultural exchanges between pupils across the world ;

  access to experts in many fields;

  access to high quality professional development for teachers;

  professional collaboration;

  exchange of pupil data with outside bodies to inform the school;

  provision of personalised learning;

Internet use at Norton Knatchbull should be focused on enhancing learning, and all teachers should plan to reinforce messages of good practise with regards to internet use :

- Teachers should provide students with clear objectives for using the internet and ensure students know what is acceptable and what is not - teachers should never assume this is already known ;
- Students must ensure that access to copyright material and its subsequent use complies with copyright law
- The school will review access levels for staff and students to reflect curriculum requirements and age of students ;
- Teachers will teach students to be critically aware of materials they access using the internet and show how to validate information before accepting its accuracy
- Teachers will ensure students are aware of restrictions in the use of AI content (see section below)

Managing school data and information systems

ICT security is a complex matter and all members of the school must play their part in ensuring that information is secured from unauthorised access. This applies to the Local Area Network (LAN) within the school as well as from the Wide Area Network to which the school is connected :

- All users must act responsibly in their network use. Persistent flouting by school staff of electronic use policy is regarded as a reason for dismissal.
- Users should take no deliberate actions to harm or compromise the network

The school will ensure that its servers are maintained in a secure environment, that adequate virus protection is employed, that workstations and servers are kept up to date and that reasonable precautions are employed to prevent accidental user mistakes.

Portable devices allow the transfer of information, and where this comprises non-personal information, all users should ensure they employ methods to allow lost data to be returned to them - ie ensure the root directory of a memory stick, or drive-name identifies the user.

All users, but especially staff must ensure that any data carried on portable devices which identifies individuals or contains data about other individuals (students or staff) of a personal nature are protected, at least using BitLocker encryption. The Computing Department can advise on how to protect documents in this way. This applies to mark-books, personnel records, letters and performance management records. It does not apply to educational resources such as powerpoint presentations. No teaching staff should hold personal data such as photos or addresses of students/parents.

All users will be aware that storing files on the school network means that these files will be accessible and potentially searched. The school has a duty to regularly check files stored on its systems - especially files which may contain illegal content such as copyright material, or those that are using a disproportionate amount of disc space. The school aims to comply with the Regulation of Investigatory Powers Act, in that access to individual users' files will only take place through generalised searches of servers, not the viewing of individual users' files or email except where general searches or other evidence indicate a reasonable need for such access, at the discretion of the Head Teacher. Student users will be monitored visually in their use of network computers (eg viewing live screenshots of use). Employees' network use will not be routinely viewed in this way. These principles and rules apply to any device that is permanently or temporarily connected to the school network, whether personal or the property of the school.

Managing electronic communication

Email is an essential mechanism for staff and student communication. It has direct organisational and educational benefits. However, as with all communication media, email has the potential to harm and to bypass the usual school boundaries. Use of the school email system should be for work purposes, and a school email address should not be used externally as a personal account - for example using the address when registering on non work-related websites.

Access to external email accounts within school will not be permitted for students. This is to prevent access to unregulated sites, and to ensure that students are regularly using their school email, which is vital for its efficient use. Staff should avoid using personal email accounts for work-purposes.

When using the school email system :

- pupils must immediately inform a member of staff if they receive an offensive email;
- pupils must not reveal personal details of themselves or others in an email communication, or arrange to meet anyone without specific permission of an adult
- pupils must not engage in excessive social email which can interfere with learning
- users must not forward chain messages or send messages likely to offend, or register theirs or others' email addresses with sites likely to generate unwanted emails
- pupils must take care when communicating with staff to ensure messages are concise, polite and appropriate
- staff must avoid attaching documents to email sent to multiple users (especially students) - use of shared areas and links prevent replication of documents and over-use of limited email account space ; linking to documents uploaded to the VLE allows access outside school.

Publishing content

The school's website allow documents, photos, video to be accessible from outside school. As with all promotional media, care must be taken to ensure information placed on public view shows the school in a good light and complies with the school's responsibilities for safeguarding its students.

- Images that include pupils will be considered with regard to safeguarding in the publication of images alongside student identity.
- The school cannot assume responsibility for images students or their parents knowingly post online, including on social networks linked to the school
- The school will respect the wish of parents and students who inform the school that they would prefer a photograph to be removed or who prefer images are not used.

Social networking, social media and personal publishing

Social media is a big part of young people's lives. Students have online spaces and students can publish unmediated content very easily. Social media allows students to communicate and connect positively with people with similar interests.

For responsible adults, social networking sites provide easy to use, free facilities. Pupils should be encouraged by all staff to be very wary of uploading true facts and personal information to these sites and to take security seriously by maintaining strong passwords and permissions. Having social spaces which their known friends can view, sharing information is very different from uploading content that anyone can view. Students should be aware that deleting content is no guarantee that content has not been archived or copied, and that such content may be found, for example by future employers.

Many social sites have age limits - for example, it is unlawful to use a Facebook account below the age of 13 as this would breach terms and conditions of use. Other services, such as Google, have restricted parent-authorised use below the age of 13. For others, such as WhatsApp, the age restriction is 16. The school will limit access to sites which have age restrictions.

- Staff should run official educational sites or blogs through the school only with authorisation from the SLT - no personal sites should be used for professional purposes without authorisation
- Students should be advised to ensure their social networking accounts are secure and that they should make sure they only allow friends to access information and photos - and how to block users.

- Staff should be aware of potential professional and personal risks in using social networking (and web publishing) and take appropriate care. For example, it is advised that adding existing students or recent leavers as accepted contacts on social networking sites may pose a potential risk. However, ex-students without siblings at the school or from schools outside Kent might be considered appropriate contacts.

Staff should make an informed decision, depending on the material they publish and check with their line manager if they are concerned.

Internet filtering

The school recognises 3 key areas of risk within online safety (Keeping Children Safe in Education 2019):

Content: being exposed to illegal, inappropriate or harmful material; for example pornography, fake news, racist or radical and extremist views;

Contact: being subjected to harmful online interaction with other users; for example commercial advertising as well as adults posing as children or young adults; and

Conduct: personal online behaviour that increases the likelihood of, or causes, harm; for example making, sending and receiving explicit images, or online bullying.

To limit children's exposure to the above risks from the school's IT system the school has appropriate filters and monitoring systems in place.

The internet connection that the school contracts with Virginmedia employs a filtering system called SmoothWall. This system uses industry standard methods of filtering content and as a secondary school, we have access to our own filtering capabilities, both adding to our own "banned-list" and enabling content through our "allow-list".

- The school will work with its broadband provider to ensure the systems protect pupils from inappropriate content as far as possible
- Staff or pupils who discover unsuitable content must report the URL directly to the ICT Support Team
- The school may apply filtering appropriate to groups of users, eg 7-11, Sixth Form, Staff.

If staff wish to check that sites they wish students to access can be accessed, they can request temporary use of a dummy student account to which standard student blocking is applied.

Emerging technologies

No policy on appropriate use of technology can take account of the continuous development of devices. The school will look at and develops its educational use of such technologies, and will be supportive of staff and students that wish to make positive innovative use of emerging technologies.

- Emerging technologies will be examined for educational benefit and a risk assessment be carried out before general use in school is encouraged.

The use of AI

Generative AI models (especially those that produce text and images) have seen rapid growth in recent years. These can be used to produce text, images and code from text-based prompts and questions. Whilst in its infancy, AI is a potentially transformative technology that is likely to form a bigger and more common part of everyday life as well change the work-lives of our staff and students in the future.

AI can support learning, especially in research and summarising long content. However, it also presents challenges. There are concerns about how AI selects and authenticates the origin of work, can exacerbate existing stereotypes or bias as well as the accuracy and reliability of content it presents as definitive answers or fact. AI Language models can generate results that are convincing but factually incorrect.

Any content produced by AI must be reviewed for its fitness-for-purpose and edited accordingly.
At NKS we are keen to ensure our students are aware of technological changes. Through teaching and dialogue, we aim to ensure that students are taught how to use AI responsibly in their work and are attuned to both the benefits and challenges it presents.

Staff should try to:

- ensure that students are aware of developments and examples of AI in the context of their subject area
- teach AI as a formal digital literacy topic within Computing KS3 lessons, including the awareness of the limitations of large language models.
- Reinforce awareness of AI across all subjects
- explore AI and raise awareness of tools that students may choose to use as part of their learning in their subject.
- give students clear criteria for mobile tools in homework and assessed tasks.
- remind students of the formal JCQ rules on the use of AI within Non-Examined Assessments (NEAs) (distributed on an annual basis by the Examinations Officer)

Students must:

- practice good referencing and acknowledge all sources of information they use in homework or assessed work; whether they are paper-based, internet based or AI sources.
- ensure AI tools are used only in ways that are specifically permitted by their teacher
- ask their teacher if unsure what limitations are in place for use of AI for assessed work and, assume AI should not be used unless they are specifically told they can
- be cautious about the reliability of the output from AI models in terms of accuracy
- keep draft copies of their work so that they can demonstrate the evolution of their work if staff suspect work was created or plagiarised using AI.

It is important to remember that the JCQ guidance must be followed when submitting coursework, NEAs or undertaking examinations:

- Students who misuse AI such that the work they submit for assessment is not their own will have committed malpractice, in accordance with JCQ regulations, and may attract severe sanctions.
- Students must make sure that work submitted for assessment is demonstrably their own. If any sections of their work are reproduced directly from AI generated responses, those elements must be identified by the student and they must understand that this will not allow them to demonstrate that they have independently met the marking criteria and therefore will not be rewarded.

The JCQ guidance on the use of AI can be found here: https://www.jcq.org.uk/exams-office/malpractice/artificial-intelligence/

Personal data management

The school is registered with the Information Commissioner's Office to hold personal data on its students, their parents and its staff. Information must comply with the eight principles outlines in the UK General Data Protection Regulation (UK GDPR), that data must be :

- processed fairly and lawfully
- processed for specific purposes
- adequate, relevant and not excessive
- accurate and up to date
- held no longer than is necessary
- processed in line with individuals' rights
- kept secure
- transferred to other countries only with suitable security measures

All members of staff must be aware that they have to follow these principles for data they generate as well as data that the school holds centrally. Data subjects have a legal right to view all information, subject to reasonable charges for administration, held about them. Biometric data is collected to permit identification for the school catering system

Permissions and access

Users do not have an automatic right to use the school's network or its internet connection. However, the school will grant such rights unless a user demonstrates that they cannot use the network appropriately.

The school has an obligation under the Computer Misuse Act 1990 to ensure that users who do not make appropriate use of the network are restricted from access to protect all other users.

Parents and students agree to accept the school's policy on acceptable use on enrolment to the school. Staff must accept this and the school's employee codes on appropriate use as part of their contract of employment.

From time to time, guest users such as visitors, PGCE students etc, may be provided with network access. The school will expect such users to understand and follow the same principles as other users.

- The school will take all reasonable precautions to ensure students are only exposed to appropriate material but the global and connected nature of internet content means that removal of risk is not possible, and that students who actively search for inappropriate content (and are therefore breaking the school's acceptable use policy) cannot be protected.
- The school will regularly review practical implementation of this policy to ensure adequate protection.
- The use of computer systems without permission or for inappropriate purposes, with the intent to cause harm, constitutes a criminal offence under the Computer Misuse Act 1990
- Complaints over inappropriate activity using our computer network will be dealt with within lessons and outside lessons according to the school's published behavioural policy aligned to similar offences
- Cyberbullying will be treated alongside other forms of bullying and dealt with according to the school's policy - as with bullying using other methods, serious issues may involve senior staff and/or outside agencies.

Inappropriate use may require senior staff to authorise period network-restrictions for individual students. Such restrictions should impact on the student’s unsupervised access to the network, not their lessons. Staff have the capability to allow students to have closely supervised access to the network whilst a restriction is in place, to ensure that teaching and learning can continue, then block at the end of the lesson.

Online Classes in Microsoft 365

MS365 has become an integral part of many subject areas' day to day work, and all departments have some level of presence on this online classroom environment.

MS365 provides teachers and departments with the ability to :

- share resources such as presentations, documents and links online
- create courses / online schemes of work via Teams which are constantly growing & evolving yet can be coherently accessed by teachers and students
- view submission of draft and final work from students, rather than managing this themselves using Teams Assignments and Show My Homework
- bind formative feedback to submitted work
- test online for informal and formal assessment
- set up forums, wikis and other methods of student-student or student-teacher dialogue
- provide differentiated resources and personalised learning - for example, learning resources suitable for students who have missed lessons

In using MS365 Students benefit from

- anytime/anywhere access to learning resources
- the ability to find additional help with work when they need it
- an online place to store (backup) assignments
- coherent and easy-to-find formative feedback of their submitted work
- the ability to interact with teachers and other students on topics in a variety of ways

MS365 also provides key whole-school services, for disseminating information, holding documents which can be accessed over the web and providing training materials.

The school will

- hold Microsoft Education to account to ensure Microsoft 365 operates on a stable and reliable platform, properly backed up and secure from external attack
- maintain levels of internet access to ensure the service is available externally as well as internally
- ensure systems are in place to maintain the information and structure of Microsoft 365 and provide non-teacher time to the administrative tasks necessary to this.

The use of Satchel:One

The school uses Satchel:One in a number of ways to

- provide students with details of homework tasks
- communicate the completion of homework
- allow homework-based teacher-student interaction
- provide tasks for occasions when the class teacher is not present

- provide work remotely to many students who are absent from class
- provide a platform for quick distribution of remote learning activities

Students should access Satchel One at least daily and ensure they are up to date with tasks they have been set. Students can access the web app using any browser, or download the app from their device's app-store.

Parents can also use their PIN to attach their NKS child to their parental account on Satchel One, and this allows access to their child's tasks and completion.

How e-safety is communicated

The communication of E-Safety is the responsibility of every member of staff in the school. However, there are formal measures in place to ensure this issue is formally addressed with students.

All year groups undertake activities and assemblies focused on E-Safety during the school year. New students receive formal e-safety training in Computing lessons in Year 7. All students spend a lesson discussing the big picture of the issues and learning the formal structures and mechanisms in place to protect them : appropriate uses, things to watch out for and how to report concerns.

Further in Years 7, 8 and 9, the Computing course develops principles of effective web searching, plagiarism and copyright. Throughout their formal courses, the issues are revisited whenever the opportunity arises. All students in Years 10 and 11 are given the opportunity to complete the Inspiring Digital Enterprise Award (IDEA) which has as a core foundation of its many digital "badges", courses focused on Digital Literacy and E-Safety.

New students into the sixth form are given details of the school's policy and e-safety issues (which are different for students nearing adulthood) when their accounts are set up on the network.

Through students' experience of ICT across the curriculum, staff should ensure they reinforce and model e-safety and appropriate use. By modelling, it is important that students are actively challenged on the issues of copyright theft – for example, it would be inappropriate for a teacher to indicate that they have copies of content for which they do not have the right or permission to reproduce. Staff are reminded of these requirements and have been required to review e-learning policies and best-practice as part of their Safeguarding annual training. The DfE document: "Teaching Online Safety in Schools, June 2019" has been made mandatory reading for all staff. Additional online safety training sessions are regularly attended by DSLs, as recommended and/or provided by the Kent Education Safeguarding Service. Additional sessions are sometimes developed for students, staff and parents. Whole school sessions for all students with an external provider take place on regular occasions.

Teachers should rigorously reinforce anti-plagiarism and copyright issues when doing research or introducing coursework. Only with a consistent approach to this can the issues be effectively learned and understood.

Storage:
All work should be stored on Sharepoint (and other school based systems such as Arbor). USB storage of any kind is not permitted. * Approval from the Network Manager must be obtained prior to transferring of files using third parties cloud storage systems (Only Microsoft OneDrive is approved for use).

When sharing documents or folders, care must be taken before switching access to “Edit” mode – the default is “View only” to limit accidental modification of documents without permission.

* Exceptionally teaching devices in the Art and DT Departments may be used for the purpose of uploading photographs from card readers only and Computing to allow the use of programming dongles.

Appendix 1 : The Legal Framework

This section is designed to inform users of potential legal issues relevant to the use of electronic communications. It is not professional advice. Many young people and indeed some staff use the internet regularly without being aware that some of the activities they take part in are potentially illegal. The law is developing rapidly and changes occur frequently.

Racial and Religious Hatred Act 2006

This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people based on their race, nationality or ethnic background.

Criminal Justice Act 2003

Section 146 of the Criminal Justice Act 2003 was enacted in April 2005 giving courts tougher sanctions for offences motivated by a victim's sexual orientation.

Sexual Offences Act 2003

This Act makes it an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of anyone under the age of 18. Viewing an image falls under this act and includes constructed pseudo-photographs (digitally constructed or otherwise), and includes images taken and distributed by the child themselves.

A person convicted of such an offence may face a prison sentence of up to 10 years.

More can be found at www.teachernet.gov.uk

Communications Act 2003 (section 127)

Sending by means of the internet a message that is grossly offensive, indecent, obscene or menacing, or causes annoyance, inconvenience or needless anxiety is an offence under the act. There is no need to prove intent – the effect of the message determines the offence.

The UK General Data Protection Regulation (UK GDPR) (GDPR)

Detailed earlier in this document. Sets rules for the retention and security of personal data.

Computer Misuse Act 1990 (Sections 1-3)

Detailed earlier. Regardless of an individual's motivation, makes it an offence to gain access to, use or impair the operation of a computer system.

Malicious Communications Act 1988 (section 1)

Similar in scope to the Communications Act above.

Copyright, Design and Patents Act 1988

Copyright is the right to prevent others from copying or using his or her “work” without permission. “Work” is something that requires skill or judgement. If created during the course of employment, copyright is held by an individual’s employer. It is an infringement of copyright to copy all or part of anyone’s work without obtaining permission. Infringement of this act is treated as theft, whether or not physical goods have been copied – ie digital media copying is theft of “work”.

Regulation of Investigatory Powers Act 2000

This Act regulates the interception of communication without knowledge or consent. This ensures compliance with the Human Rights Act 1998.

However, monitoring and record keeping to ensure compliance with communication policy or authorised use of the network is permitted under the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, but all parties must have knowledge that such monitoring routinely takes place.

Education and Inspections Act 2006

Provides that head teachers have the power “to such an extent as is reasonable” to regulate the conduct of pupils off the school site. This is important in being able to deal with issues of cyberbullying, as these actions often take place outside school hours but have an effect in school.

The Act also provides that school staff are able to confiscate items such as mobile phones when they are being used to cause a disturbance in class or contravene the school behaviour policy.

Appendix 2 : Students – The code of Acceptable Use

In using the network facilities NKS provides, students recognise the great benefit that access to ICT facilities and the internet brings to learning. Students must periodically acknowledge that they are familiar with, and agree with, the terms below :

- I will only use my own login, email address and password, which I will not share with others
- I will not access anyone else's work on the network without their permission • I will not attempt to download or install software, shareware or freeware on the network either directly or via portable devices
- I will not attempt to violate copyright laws or licensing agreements
- I will avoid plagiarism by not passing off work downloaded from the internet as my own or use work I know was produced by somebody else. I will give clear references to sources where I have downloaded someone else's work
- I will use ICT facilities and the internet for classwork and homework, not personal use
- I will not attach any device to the network which may contain files which breach copyright, data protection or other laws
- I will not play computer games during the school day unless I have been directed to do so by a member of staff to support my learning, or using my own device (as permitted outside lesson time).
- I will not use the internet without permission from a member of staff
- I will not search, view, send or display offensive or time-wasting materials
- I will not send offensive, threatening or time-wasting messages nor post inappropriate images on websites
- I will only print copies of my work when it is really necessary. I will reduce my printing by selecting pages or printing handouts. I will only print in colour when this is essential to my learning. I understand that the school will monitor any printing that I do and may take action if this is excessive.
- I will not use inappropriate chat rooms and social networking websites during the school day, nor use the School ICT facilities for personal financial gain, gambling, political purposes or advertising
- I will not give out personal information such as full name, home address, telephone numbers or personal email to anyone whose identity I cannot be certain of over the internet
- I will not arrange to meet anyone I have met over the internet, and I will notify an adult immediately if I encounter materials or messages that make me feel uncomfortable or if I suspect someone else of misusing ICT facilities or the internet
- I will respect resources and not damage or steal ICT facilities and I understand that the school will check files and monitor the internet sites used by students, I understand that sanctions will be used if I misuse ICT facilities or the internet
- I have read and understood the above statements and I agree to comply with the school's rules for use of ICT facilities and the internet. I understand that failure to do this could result in the loss of my access rights to these facilities or the internet, along with further sanctions for serious misuse.

Appendix 3 : Staff – The code of Acceptable Use

Using our network is expected in the role of all staff. As part of their terms of employment, staff must agree to follow the terms below :

- I will keep my login, email address and password confidential.
- I will take care to ensure that others cannot use my accounts to access confidential information about students or staff by always logging off when I have finished work or locking my computer when it is left unattended.
- I will not attach any device to the network which may contain files which breach copyright, data protection or other laws and I agree not to use ICT hardware from outside of the school without informing the network manager
- I agree to use the school's ICT facilities and internet are intended for work-related use during directed time.
- I will not search, view, send or display offensive materials such as pornography or use the school's ICT facilities for personal financial gain, gambling, political purposes or advertising
- All email sent will be of a professional nature and appropriate to its audience.
- I will only print copies of my work when it is really necessary. I will reduce my printing by selecting pages and use online deployment of resources (eg Office 365 and Show My Homework) where possible
- I will take care when giving out personal information, for example, to students and parents.
- I will notify my line manager if I encounter materials or messages that are inappropriate to the work of the school or if I suspect someone else of misusing ICT facilities or the internet
- I understand that I must inform the Head Teacher immediately if I suspect another member of the school of serious or illegal misuse of ICT facilities or the internet, in line with the school policy.
- I understand that I must also inform the designated Child Protection Officer if this misuse may be a child protection issue
- I will ensure that all students under my supervision use ICT facilities and the internet appropriately to support learning. I will challenge and report any misuse, and will plan the use of ICT facilities to best support students' learning. I will follow all relevant booking procedures, ensure that I escort students into and out of ICT facilities, and be considerate to other teachers in how the IT rooms are left after use.
- I will ensure that I follow relevant Health and Safety regulations when using ICT facilities such as not looking directly at the light from a projector and not leaving students unsupervised around projectors.
- I will ensure that ICT facilities are left in a fit state for the next person or class to use them
- I understand that I am responsible for the safekeeping of any ICT equipment which I use, including such equipment which I may take off site. I will not remove ICT

equipment from the site without following the signing it procedure (see the network manager)

- I understand that the network is not private, and the school may check files and monitor the internet sites used by staff
- I understand that serious misuse of ICT facilities and the internet could result in disciplinary action being taken against me.

Two Factor-authentication

The School operates two factor-authentication for staff when accessing the school network remotely.

It is not compulsory for the school to provide a device to allow Two-factor Authentication.

Access to Office 365 or any cloud software requiring Office 365 credentials (Arbor, Satchel…) is available at all times within the school premises or from home via VPN access.

Outside school, accessing these services directly will depend on two-factor authentication being enabled.

If a user declines to use Two factor authentication on their own device or because they don't own a compatible device, then they will not be able to access services from home directly and will only be able to do it indirectly via VPN access.

If the user does not want to use the VPN (or is not authorised to), then the only option will be to access the services within the school site.

The IT support team will use a device to complete the two-factor authentication for the member of staff, but will not provide codes/approvals via that device each time the user tries to login from home, this will be purely to

1. Secure the account from phishing attacks.
2. Prevent the need to skip the two-factor authentication process each time the user logs in at school

THE USE OF PERSONAL DEVICES FOR REMOTE ACCESS AND TEACHING

Staff should use school devices over personal devices wherever possible. Where it is not possible, it is permissible to use personal devices, however, the general safeguarding and IT security principles which apply when using school equipment and infrastructure continue to apply. In particular:

- Access should be via password protected accounts
- Work should not be left unattended/unlocked
- No image, video or sound recordings of students or interactions with or between students should be made or downloaded onto devices

REMOTE TEACHING

Any live virtual sessions undertaken by teachers are only to be conducted using Microsoft Teams Meetings. This decision has been arrived at, due to the fact that Teams Meetings is part of the Microsoft Office platform that the school already uses and is central to our school systems. It offers high level encryption and compliance with GDPR. The following procedures must be followed: Consent Parents/carers in the main school must give consent which outlines the following:

- Use of Teams Meetings will be monitored and logs will be kept by the school.
- All pupils can access 'Teams' through Office 365, which is connected to their school email address.
- It is the responsibility of parents to ensure students:
    - Do not record the session in any way shape or form
    - Behave appropriately during call
    - Only access and participate using audio
- Parents are advised that if students do not behave appropriately teachers have the discretion to remove them from the call

Staff Agreement

If staff are intending to carry out a live session they are agreeing to the following arrangements and must let their subject Leader and the Headteacher know:

- Sessions have to be during school hours
- No recording should be made; in Teams or onto any other device
- If students do not adhere to the rules, they are to be removed from the call and the issue reported to the Subject Leader and Headteacher.
- Meetings should never take place with just one student. This means waiting until at least 2 students are in the waiting room before starting, and if there is only one student left in a meeting it should be ended.

Staff Training Online CPD on using Teams Meetings with students, is available to staff who require it. This will involve instruction and discussion and then splitting into groups to 'test' it.

Staff should review this playlist of tips and tutorials:
https://www.youtube.com/playlist?list=PLwXXOxvDboeYk4dtLokNMFPl84setxlI8

Further advice can be sought from M Gowen.

Teams Meetings should then be carried out as shown below:

Running Teams Meetings

- Details regarding Teams Meetings should only be shared via school email and/or SMHW. Don't share details on social media.
- Ensure that pupils only access the meeting by 'signing in' using their school email address.

- Virtual waiting rooms should be used - Using this feature, the teacher holds potential participants in a separate "waiting room", so they can check who they are before allowing them entry.
- Participants (students and teachers) should not use video. Cameras should be turned off. The session should be managed via audio and screensharing. A student that refuses to turn off their video should be removed from the session.
- Students in the main school whose parents haven't given consent cannot join (staff will have access to this information)
- Mute attendees on joining to allow for a more organized start.
- At the start of every meeting, the member of staff should remind the students of the terms of the user agreement and their expectations for the session.
- Screen sharing – The teacher should control this – if the teacher starts the session sharing their screen; even if blank then this gives the teacher control and prevents students from sharing random content as other users then have to request permission to share their screen from the teacher.