West Norfolk Academies Trust

Online Safety Policy

(Incorporating the ICT security policy and the acceptable use of ICT policy and guidance)

Approved By:	Governing Body
Approval Date:	September 2023
Review Date:	September 2024

Contents

Appendices

1. Purpose and Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

1.2 The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scam

2. Legislation and guidance

2.1 This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation

2.2 It also refers to the Department's guidance on The Prevent duty: safeguarding learners vulnerable to radicalisation. It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

2.3 The policy also considers the National Curriculum computing programmes of study.

2.4 This policy complies with our funding agreement and articles of association.

3. Roles and responsibilities

The Governing Body

3.1 The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

3.2 The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety and monitor online safety logs as provided by the designated safeguarding lead (DSL).

3.3 All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 3)
- Ensure that all staff undergo safeguarding training to include online safety and that this includes an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring.
- Do all that they reasonably can to limit children's exposure potentially harmful and inappropriate online material on the school's IT system.
- Ensure schools have appropriate filtering and monitoring in place and regular review their effectiveness.
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with SEND because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

The Headteacher

3.4 The Headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

The Designated Safeguarding Lead (DSL)

3.5 Details of the schools' DSL and deputies are set out in our Safeguarding Policy as well relevant job descriptions.

3.6 The DSL takes lead responsibility for online safety and understanding the filtering and monitoring systems and procedures in place in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school.

- Working with the headteacher, Trust IT staff and other staff, as necessary, to address any online safety issues or incidents, including reviewing the effectiveness of the school's filtering and monitoring systems.
- Managing all online safety issues and incidents in line with the school child protection policy
- Ensuring that any online safety incidents are logged on CPOMS and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety ensuring that relevant staff have an awareness and understanding of the provisions in place in regards to filtering and monitoring and that they manage them effectively to know when to escalate concerns identified.
- Liaising with other agencies and/or external services if necessary.
- Providing regular reports on online safety in school, including the effectiveness of the filtering and monitoring systems to the headteacher and/or governing board.
- To be responsible for ensuring the standards in the DFE Filtering and Monitoring documentation are met.

West Norfolk Academy Trust IT Team

3.7 The WNAT IT team is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the schools' ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the schools' ICT systems on a regular basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Helping to ensure that any online safety incidents are dealt with appropriately in line with this policy
- Helping to ensure that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

All staff and volunteers

3.8 All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently

- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 3 & 4), and ensuring that pupils follow the school's terms on acceptable use (appendices 1 and 2)
- Working with the DSL to ensure that any online safety incidents are logged on CPOMS and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'
- Having an understanding of the expectations, applicable role and responsibilities in relation to filtering and monitoring

Parents

3.9 Parents are expected to:

- Notify a member of staff or the Headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendices 1 and 2)
- Support the school in their online safety approaches by discussing online safety issues with their children and reinforce appropriate, safe online behaviours at home.
- Seek help and support from the school, or other appropriate agencies, if they or their child encounter risk or concerns online.
- Use school systems, such as Google classroom, and other network resources, safely and appropriately.

Visitors and members of the community

3.10 Visitors and members of the community who use the schools' ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 4).

4. Educating pupils about online safety

4.1 It is essential that children are safeguarded from potentially harmful and inappropriate online material. We have an effective whole school approach to online safety that empowers us to protect and educate pupils, students, and staff in their use of technology and establishes mechanisms to identify, intervene in, and escalate any concerns where appropriate.

4.2 At our school we ensure online safety is a running and interrelated theme. Pupils will be taught about online safety as part of a broad and balanced curriculum:

We recognise the breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk:

- **Content:** being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.
- **Contact:** being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes'.
- **Conduct:** personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying; and
- **Commerce:** risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group (https://apwg.org/).

4.3 In Key Stage 3, pupils will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact and conduct, and know how to report concerns

4.4 Pupils in Key Stage 4 will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns

4.5 By the end of secondary school, pupils will know:

- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online
- Not to provide material to others that they would not want shared further and not to share personal material which is sent to them
- What to do and where to get support to report material or manage issues online
- The impact of viewing harmful content
- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including jail
- How information and data is generated, collected, shared and used online
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours

- How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online)

4.6 The safe use of social media and the internet will also be covered in other subjects where relevant.

4.7 Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

4.8 The school will use assemblies and other national days to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

5. Educating parents about online safety

5.1 The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents.

5.2 If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the Headteacher and/or the DSL.

5.3 Concerns or queries about this policy can be raised with any member of staff or the Headteacher.

5.4 Parents can seek further guidance on keeping children safe online from a range of organisations and websites, for example:

- https://www.thinkuknow.co.uk/parents/
- https://www.saferinternet.org.uk/advice-centre/parents-and-carers
- https://www.nspcc.org.uk/keeping-children-safe/online-safety/
- https://www.childnet.com
- https://www.internetmatters.org

6. Procedures for Responding to Specific Online Incidents or Concerns

6.1 Cyber – bullying Definition

6.1.1 Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

6.2 Preventing and addressing cyber-bullying

6.2.1 To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

6.2.2 The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be.

6.2.3 Teaching staff also find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes lessons using our e-safety curriculum (based on DfE Education for a Connected World), computing curriculum (based on NCCE lesson plans), PHSE lessons from the PHSE association and other subjects where appropriate.

6.2.4 All staff, receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

6.2.5 In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

6.2.6 The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

6.3 Consensual and non-consensual sharing of nude and semi-nude images and/or videos

6.3.1 The school recognises consensual and non-consensual sharing of nudes and semi-nudes and/or videos (also known previously as youth produced sexual imagery or “sexting”) as a safeguarding issue; therefore, all concerns will be reported to and dealt with by the Designated Safeguarding Lead.

6.3.2 The school will ensure that all members of the community are made aware of the potential consequences of consensual and non-consensual sharing of nudes and semi-nudes and/or videos by implementing preventative approaches, via a range of age and ability appropriate educational methods.

6.3.3 The school will ensure that all members of the community are aware of sources of support regarding youth produced sexual imagery.

6.3.4 If the school are made aware of an incident involving the creation or distribution of youth produced sexual imagery, the school will act in accordance with our Child Protection and Safeguarding policies and Behaviour Policies

6.3.5 In line with DFE guidance: Sharing nudes and semi nudes: advice for education settings working with children and young people, if a member of staff is alerted to an incident they know, or suspect, is a nude or semi-nude picture they must never view, copy, print, share, store or save the imagery themselves, or ask a child to share or download – this is illegal.

6.3.6 The DSL will make a referral to children’s social care and/or the police immediately if there is a concern that a child or young person has been harmed or is at risk of immediate harm at any point in the process.

6.4 Online Child Sexual Abuse and Exploitation

6.4.1 The school will ensure that all members of the community are aware of online child sexual abuse, including: exploitation and grooming; the consequences; possible approaches which may be employed by offenders to target children and how to respond to concerns.

6.4.2 The school recognises online child sexual abuse as a safeguarding issue and, as such, all concerns will be reported to and dealt with by the Designated Safeguarding Lead.

6.4.3 The school will implement preventative approaches for online child sexual abuse via a range of age and ability appropriate education for pupils, staff and parents/carers.

6.4.4 The school will ensure that all members of the community are aware of the support available regarding online child sexual abuse, both locally and nationally.

6.4.5 The school will ensure that the 'Click CEOP' report button is visible and available to pupils and other members of the school community through the school's website

6.5. Dealing with Online Child Sexual Abuse and Exploitation

6.5.1 If the school are made aware of incident involving online sexual abuse of a child, the school will act in accordance with the school's Child Protection and Safeguarding Policies

- Immediately notify the Designated Safeguarding Lead.
- Store any devices involved securely.
- Immediately inform police via 101 (or 999 if a child is at immediate risk)
- Carry out a risk assessment which considers any vulnerabilities of pupil(s) involved (including carrying out relevant checks with other agencies).
- Inform parents/carers about the incident and how it is being managed.
- Provide the necessary safeguards and support for pupils, such as, offering counselling or pastoral support.
- Review the handling of any incidents to ensure that best practice is implemented; school leadership team will review and update any management procedures, where necessary.

6.5.2 The school will take action regarding online child sexual abuse, regardless of whether the incident took place on/off school premises, using school or personal equipment.

6.5.3 Where possible pupils will be involved in decision making and if appropriate, will be empowered to report concerns such as via CEOP

6.5.4 If the school is unclear whether a criminal offence has been committed, the DSL will obtain advice immediately through the CADS and Norfolk Safeguarding Children Partnership.

6.5.5 If the school is made aware of intelligence or information which may relate to child sexual exploitation (on or offline), it will be passed through to the CADS by the Designated Safeguarding Lead.

6.5.6 If pupils at other schools are believed to have been targeted, the school will seek support from Police and/or the Education Safeguarding Team first to ensure that potential investigations are not compromised.

6.6 Examining electronic devices

(This should be read in conjunction with the Trust Staff Code of Conduct: Section 18. Unacceptable Use of ICT Facilities and Monitoring)

6.6.1 School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

6.6.2 When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules
- If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:
- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police

6.6.3 Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation.

6.6.4 Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

7.1 Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1-3). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant. More information is set out in the acceptable use agreements in appendices 1, 2 and 3.

7.2 Internet access, security and filtering

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role. In our schools we follow guidelines issued by the Department for Education to ensure that we comply with minimum requirements in the filtering and monitoring standards.

7.3 E-mail

7.3.1 We provide staff with an email account for their professional use and make it clear that personal email should be through a separate account

7.3.2 We use anonymous e-mail addresses, for example head@, office@

7.3.3 Will contact the Police if one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law.

7.3.4 Will ensure that email accounts are maintained and up to date

7.4 Pupils email:

7.4.1 We use school provisioned pupil email accounts that can be audited and which do not identify the child in the email address itself.

7.4.2 Pupils are taught about the online safety and ‘etiquette’ of using e-mail both in school and at home.

7.4.3 Pupils will sign an Acceptable Use Agreement and will receive education regarding safe and appropriate email etiquette before access is permitted.

7.5 Staff email:

7.5.1 Staff will use Trust or school provisioned e-mail systems for professional purposes

7.5.2 Access in school to external personal e-mail accounts may be blocked

7.5.3 Staff will not use email to transfer staff or pupil personal data unless it is protected with secure encryption. ‘Protect-level’ data should never be transferred by email. If there is no secure file transfer solution available for the situation, then the data / file must be protected with security encryption.

7.6 School websites

7.6.1 The school’s website complies with statutory DfE requirements.

7.6.2 Most material is the schools’ own work; where others’ work is published or linked to, we credit the sources used and state clearly the author's identity or status;

7.6.3 Photographs of pupils published on the web do not have full names attached. We do not use pupils’ names when saving images in the file names or in the tags when publishing to the school website;

7.6.4 The school will post information about safeguarding, including online safety, on the website;

7.6.5 We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above. (See Staff Code of Conduct Section 17)

7.7 Management Information System access and data transfer

7.7.1 Teachers and office staff have access to the MIS (SIMS).

7.7.2 Data on this system must not be copied or shared with any other person and kept confidential.

7.7.3 Staff must log out of the MIS or ‘lock’ the machine when they are not near the computer.

7.8 Social networking - Staff, Volunteers and Contractors

7.8.1 The use of any school approved social networking (e.g School Twitter Account or School Facebook account) will adhere to ICT Acceptable Use Agreement

7.8.2 Staff will not use personal social media accounts to make contact with pupils or parents, nor should any contact be accepted, except in circumstance whereby prior approval has been given by the Executive Headteacher.

7.8.3 All members of staff are advised not to communicate with or add as ‘friends’ any current or past pupils or current or past pupils’ family members via any personal social media sites, applications or profiles.

7.8.4 Any pre-existing relationships or exceptions that may compromise this will be discussed with Designated Safeguarding Lead and/or the Headteacher.

7.8.5 If ongoing contact with pupils is required once they have left the school roll, members of staff will be expected to use official school provided communication tools.

7.9 Digital images and video

7.9.1 We gain parental/carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter/son joins the school

7.9.2 We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials/DVDs

7.9.3 Staff sign the school’s Acceptable Use Agreement and this includes a clause on the use of personal mobile phones/personal equipment

Pupils:

Are taught about social networking, acceptable behaviours and how to report misuse, intimidation or abuse through our online safety curriculum work. Students are required to sign and follow our pupil Acceptable Use Policy (Appendix 1 and 2)

Parents/Carers:

Parents/carers are reminded about social networking risks and protocols through our Acceptable Use Policy and additional communications materials when required.

Communicating with Pupils, Parents and Carers

School will communicate with parents via approved official channels e.g. school website, email, school Twitter account etc. All communication will comply with the Trust Data Protection Policy and Privacy Notices.

8. Bring Your Own Device Guidance for Staff and Pupils

8.1 Pupils personal devices *(smartphones, laptops, personal tablets etc.)* should not be connected to the schools' Wi-Fi.

- Pictures of children should not be taken on personal devices.
- Personal devices, other than smartphones, are discouraged from being brought into school.
- If a personal laptop is brought into school to use a BOYD must be signed by both parent and student.

8.2 Pupils using mobile devices in school

- Pupils may bring a mobile device into school. Mobile phones must be switched off and in bags during the day.
- Any use of mobile devices in school by pupils must be in line with the acceptable use policy.
- Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of the device.

9. Staff using work devices outside school

9.1 All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- If staff have any concerns over the security of their device, they must seek advice from the Trust ICT technician
- Keeping operating systems up to date – always install the latest updates

9.2 Staff members must not use the device in any way which would violate the school's terms of acceptable use.

10. How the schools will respond to issues of misuse (Also see Staff Code of Conduct)

10.1 Where a pupil misuses the school's ICT systems or internet, we will follow the procedures, in line with current guidance from the Department for Education, as set out in our policies on Behaviour, and Internet Acceptable Use Policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

10.2 The DSL acts as the first point of contact for any safeguarding incident whether involving technologies or not.

10.3 Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with by the Headteacher, in accordance with the Staff Disciplinary Procedures and Staff Code of Conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

10.4 In our schools:

- there is strict monitoring and application of the Online Safety Policy, including the ICT Acceptable Use Policy and a differentiated and appropriate range of sanctions
- support is actively sought from other agencies as needed *(i.e. the local authority, UK Safer Internet Centre helpline, CEOP, Police)* in dealing with online safety issues
- monitoring and reporting of online safety incidents takes place and contribute to developments in policy and practice in online safety within our schools
- parents/carers are specifically informed of online safety incidents involving young people for whom they are responsible
- the Police will be contacted if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law
- we will immediately refer any suspected illegal material to the appropriate authorities – i.e. Police, Internet Watch Foundation and inform the Trust
- for any breach of the acceptable use policy, the school will follow the agreed sanctions described in appendix 5 of this policy
- The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

11. Training

11.1 All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including filtering and monitoring, cyber-bullying and the risks of online radicalisation.

11.2 All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

11.3 The DSL deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

11.4 Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

11.5 Volunteers will receive appropriate training and updates, if applicable.

11.6 More information about safeguarding training is set out in our child protection and safeguarding policy.

12. Monitoring arrangements

12.1 The DSL logs behaviour and safeguarding issues related to online safety on CPOMS.

12.2 This policy will be reviewed every annually by the Designated Safeguarding Lead. At every review, the policy will be shared with the governing board.

13. Other relevant policies

- Safeguarding and Child Protection Policy
- Behaviour policy
- Staff Code of Conduct
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- Acceptable use policy

Appendix 1: Pupil Acceptable Use Policy

Safe

- I only send messages which are polite and friendly
- I will only post pictures or videos on the internet if they are appropriate and if I have permission
- I only talk with and open messages from people I know, and I only click on links if I know they are safe
- I know that people I meet online may not always be who they say they are. If someone online suggests meeting up, I will immediately talk to an adult

Trust

- I know that not everything or everyone online is honest or truthful
- I will check content on other sources like other websites, books or with a trusted adult
- I always credit the person or source that created any work, image or text I use

Responsible

- I always ask permission from an adult before using the internet
- I only use websites and search engines that my teacher has chosen
- I use school computers for school work, unless I have permission otherwise
- I know that personal devices are not permitted in school
- I keep my personal information safe and private online
- I will keep my passwords safe and not share them with anyone
- I will not access or change other people's files or information
- I will only change the settings on the computer if a teacher/technician has allowed me to

Understand

- I understand that the school's internet filter is there to protect me, and I will not try to bypass it.
- I know that my use of school devices/computers and internet access will be monitored
- I have read and talked about these rules with my parents/carers
- I can visit www.thinkuknow.co.uk and www.childline.org.uk to learn more about keeping safe online
- I know that if I do not follow the school rules then I will receive a sanction

Tell

- If I am aware of anyone being unsafe with technology, I will report it to a teacher
- I always talk to an adult if I'm not sure about something or if something happens online that makes me feel worried or frightened
- If I see anything online that I shouldn't or that makes me feel worried or upset then I will minimise the page, shut the lid and tell an adult straight away

We request that children at our school sign and return the agreement form to ensure that we respect the rules around online safety. This is a safeguarding matter which will benefit everyone.

West Norfolk Academies Trust

Acceptable Use Policy - Pupil Response

I, with my parents/carers, have read and understood the pupil Acceptable Use Policy (AUP).

I agree to follow the pupil AUP when:

1. I use school systems and devices, both on and offsite
2. I use my own equipment out of the school, in a way that is related to me being a member of the school community, including communicating with other members of the school, accessing school email, learning platform or website.

Pupil name………………………………………………. Signed……………………….

Form………………………… Date…………………….

School …………………………………………………

Parents Name………………………………………….......

Parents Signature………………………… …………………….

Date…………….

Appendix 2: Parent/Carers Acceptable Use Policy

1. I have read and discussed the School Acceptable Use Policy with my child.
2. 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 school.
3. I am aware that any internet and computer use using school equipment may be monitored for safety and security reasons, to safeguard both my child and the schools' systems. This monitoring will take place in accordance with data protection (including GDPR) and human rights legislation.
4. I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.
5. I understand that if the school has any concerns about my child's safety online, either at school or at home, then I will be contacted.
6. I understand that if my child does not abide by the school Acceptable Use Policy then sanctions will be applied in line with the school policies including behaviour, online safety and anti-bullying policy. If the school believes that my child has committed a criminal offence, then the Police will be contacted.
7. I, together with my child, will support the school's approach to online safety 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 school community. I will not share other pupils work on social media.
8. I know that I can speak to the school Designated Safeguarding Lead, my child's pastoral manager or the headteacher if I have any concerns about online safety.
9. I will visit the school website for more information about the school's approach to online safety as well as to access useful links to support both myself and my child in keeping safe online at home.
10. I will visit the following websites for more information about keeping my child(ren) safe online:
    - www.thinkuknow.co.uk/parents,
    - www.nspcc.org.uk/onlinesafety
    - www.internetmatters.org
    - www.saferinternet.org.uk
    - www.childnet.com

11. I will support the school and my child by role modelling safe and positive online behaviour (such as sharing images, text and video responsibly) and by discussing online safety with them when they access technology at home.

West Norfolk Academies Trust

Acceptable Use Policy - Parent Response

I have read, understood and agree to comply with the School Acceptable Use Policy (AUP).

Pupil name……………………………………………Form……………… Date…………………….

School ………………………………………………………………………………………..

Parents Name…………………………………………………………………….......

Parents Signature…………………………. ……………………. Date…………….

Appendix 3: Staff Acceptable Use Policy

As a professional organisation with responsibility for safeguarding, it is important that staff take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft. All members of staff have a responsibility to use the school's computer system in a professional, lawful, and ethical manner. To ensure that members of staff are fully aware of their professional responsibilities when using technology, they are asked to read and sign this Acceptable Use Policy.

This is not an exhaustive list; all members of staff are reminded that IT use should be consistent with the school ethos, school policies, national/local guidance and expectations, and the Law.

1. I understand that Information Systems and IT include networks, data and data storage, online and offline communication technologies and access devices. Examples include laptops, mobile phones, tablets, digital cameras, email and social media sites**.**

2. School owned information systems must be used appropriately. I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.

3. I understand that any hardware and software provided by my workplace for staff use can only be used by members of staff and only for educational use. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or locking my login as appropriate. I will protect the devices in my care from unapproved access or theft.

4. I will respect system security and will not disclose any password or security information. I will use a 'strong' password to access school systems. A strong password has numbers, letters and symbols, with 8 or more characters, does not contain a dictionary word and is only used on one system.

5. I will not attempt to install any purchased or downloaded software, including browser toolbars, or hardware without permission from the system manager.

6. I will ensure that any personal data of pupils, staff or parents/carers is kept in accordance with the Data Protection legislation (including GDPR).
   - This means that all personal data will be obtained and processed fairly and lawfully, only kept for specific purposes, held no longer than necessary and will be kept private and secure with appropriate security measures in place, whether used in the workplace, hosted online or accessed remotely.
   - Any data being removed from the school site (such as via email or on memory sticks or CDs) will be suitably protected. This may include data being encrypted by a method approved by the school.
   - Emails used for school business must be official work emails and not personal emails

  - Any images or videos of pupils will only be used for school business and will always reflect parental consent.

7. I will not keep documents which contain school-related sensitive or personal information, including images, files, videos and emails, on any personal devices, such as laptops, digital cameras, and mobile phones. Where possible, I will use the school google drive to upload any work documents and files

8. I will not store any personal information on the school computer system including any school laptop or similar device issued to members of staff that is unrelated to school activities, such as personal photographs, files or financial information.

9. I will respect copyright and intellectual property rights.

10. I have read and understood the school online safety policy which covers the requirements for safe IT use, including using appropriate devices, safe use of social media and the supervision of pupils within the classroom and other working spaces.

11. I will immediately report any illegal, inappropriate or harmful material or incidents I become aware of, to the Designated Safeguarding Lead.

12. I will not attempt to bypass any filtering and/or security systems put in place by the school. If I suspect a computer or system has been damaged or affected by a virus or other malware, or if I have lost any school related documents or files, I will report this to the Trust ICT Team as soon as possible.

13. My electronic communications with current or past pupils, parents/carers and other professionals will take place within clear and explicit professional boundaries and will be transparent and open to scrutiny.
    - All communication will take place via school approved communication channels, such as a school provided email address, Class Dojo or telephone number, and not via my personal devices or communication channels, such as personal email, social networking or mobile phones.
    - Any pre-existing relationships or situations that may compromise this will be discussed with the Headteacher.

14. I will ensure that my online reputation and use of IT and information systems are compatible with my professional role, whether using school or personal systems. This includes the use of email, text, social media, social networking, gaming and any other devices or websites.
    - I will take appropriate steps to protect myself online as outlined in the Online Safety Policy and will ensure that my use of IT and the internet will not undermine my professional role, interfere with my work duties and will be in accordance with the Trust Code of Conduct/Behaviour Policy and the Law.

15. I will not create, transmit, display, publish or forward any material online that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring my professional role, the school, or the County Council, into disrepute.

16. I will promote online safety with the pupils in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create.

17. If I have any queries or questions regarding safe and professional practise online either in school or off site, I will raise them with the Headteacher.

18. I understand that my use of the school information systems, including any devices provided by the school, including the school internet and school email, may be monitored and recorded to ensure the safety of children and staff and to ensure policy compliance. This monitoring will be proportionate and will take place in accordance with data protection, privacy and human rights legislation.

19. I understand that the school may exercise its right to monitor the use of information systems, including internet access and the interception of emails, to monitor policy compliance. Where it believes unauthorised and/or inappropriate use, or unacceptable or inappropriate behaviour may be taking place, the school may invoke its disciplinary procedures. If the school suspects criminal offences have occurred, the matter will be brought to the attention of the relevant law enforcement organisation.

20. I understand my role and responsibilities in relation to filtering and monitoring and understand the provisions that are in place to manage them effectively and know how to escalate concerns when identified.

I have read, understood, and agreed to comply with the School Staff Acceptable Use Policy.

Name .... Signed..

Date:...

Appendix 4: Visitor/Volunteer Acceptable Use Policy

As a professional organisation with responsibility for children's safeguarding it is important that all members of the community, including visitors and volunteers, are fully aware of their professional responsibilities and read and sign this Acceptable Use Policy.

This is not an exhaustive list; visitors/volunteers are reminded that ICT use should be consistent with the school ethos, other appropriate school policies, relevant national and local guidance and expectations, and the Law.

1. I will ensure that any personal data of pupils, staff or parents/carers is kept in accordance with Data Protection legislation, including GDPR. Any data which is being removed from the school site, such as via email or on memory sticks or CDs, will be encrypted by a method approved by the school. Any images or videos of pupils will only be used as stated in the school image use policy and will always reflect parental consent.

2. I have read and understood the school online safety policy which covers the requirements for safe ICT use, including using appropriate devices, safe use of social media websites and the supervision of pupils within the classroom and other working spaces.

3. I will follow the school's policy regarding confidentially, data protection and use of images and will abide with copyright and intellectual property rights, child protection legislation, privacy and data protection law and other relevant civil and criminal legislation.

4. My electronic communications with pupils, parents/carers and other professionals will only take place within clear and explicit professional boundaries and will be transparent and open to scrutiny.
    - All communication will take place via school approved communication channels such as via a school provided email address or telephone number and not via personal devices or communication channels such as via personal email, social networking or mobile phones.
    - Any pre-existing relationships or situations that may compromise this will be discussed with the Designated Safeguarding Lead and/or Headteacher.

5. My use of ICT and information systems will be compatible with my role within school. This includes the use of email, text, social media, social networking, gaming, web publications and any other devices or websites. I will take appropriate steps to protect myself online and my use of ICT will not interfere with my work duties and will always be in accordance with the school AUP and the Law.

6. I will not create, transmit, display, publish or forward any material that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring my professional role, the school, or the County Council, into disrepute.

7. I will promote online safety with the children in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create.

8. If I have any queries or questions regarding safe and professional practise online either in school or off site, I will raise them with the Designated Safeguarding Lead or the Headteacher.

9. I will report any incidents of concern regarding children's online safety to the Designated Safeguarding Lead as soon as possible. They can be contacted:

10. I understand that if the school believes inappropriate use or unacceptable behaviour is taking place, the school may invoke its disciplinary procedure. If the school suspects criminal offences have occurred, the matter will be brought to the attention of the relevant law enforcement organisation.

I have read, understood and agree to comply with the School's Visitor / Volunteer Acceptable Use Policy.

Name:…………………………………………… Signed:…………………………………………

Date:……………………………………………..

Appendix 5: Sanctions for unacceptable use

Sanctions for unacceptable use

- Parents will be informed as soon as possible
- A temporary or permanent ban from Internet access
- A temporary or permanent ban from the use of school's ICT facilities
- Access to the Internet may be withdrawn.
- A serious breach of the policy will result in further disciplinary action being taken, including exclusion.
- If it is suspected that a criminal offence has been committed the appropriate authorities will be informed
- Appropriate additional disciplinary action if the action breaks any other school rule or convention.
- This action will be defined in the other policies:
    - Whole School Behaviour Policy
    - Anti-bullying Policy
- Where applicable, referral to appropriate external agencies.

Appendix 6: ICT security

Concerns and Risks

- Any removable storage used from home may contain a virus. Accessing the Internet and downloading could contain a virus.
- Users staying logged on and leaving machines could allow access to files by unauthorised person(s).
- Disks containing confidential records left in machines after use. Unauthorised user(s) obtaining staff passwords.
- Users installing unauthorised or unlicensed software. Data being changed or deleted by unauthorised user(s).
- Users unaware of the legal responsibilities when using software or when recording data.

Security Responsibilities/Procedures Virus checking

Students are actively encouraged to transfer work from home. However, students in Years 7 to 11 do not have access to removable media and are encouraged to use the school’s email system to complete this task. If removable media from home is used the student should take the media to the ICT Support Team for the work to be transferred. All PC’s in the school have up to date anti-virus software and any removable media is automatically scanned.

Our connection to the Internet is via BT which includes a secure connection by a filtering system and virus checking.

The school’s email system is provided by Google and includes virus checking.

General procedures

1. Logging on and logging off

   All staff will need to log on using their own username and a password. Staff should ensure that during log on procedure they do not allow others to access their password. Passwords should not be written down. If passwords are obtained by others, they should be changed immediately. Once a session is ended users should log off; machines should not be left unattended and logged in. If a member of staff leaves a machine, it should be locked.

2. Administration Files

   Staff will have a security level, which will allow access only to appropriate areas of the Management Information System (SIMS.et). If the appropriate level has not been set staff should inform the ICT Systems Manager. After log on staff have access to a drive labelled Q: Staff Documents, which only staff can access. Staff files should be stored in a Google shared drive.

3. Use of removable storage

   If removable storage is used to copy details from school to home the appropriate levels of confidentiality and security are to be employed. Users should ensure that removable storage items are not left in PCs after use or where unauthorised users have access to it.

4. Access From Home

   Access to the school network is provided by a secure VPN connection using L2TP/IPsec with pre-shared key protocol, using AES 256-bit encryption. Each staff member is given a unique username and a complex password to prevent any password guessing from an unknown source.

5. Curriculum

Staff can create files that students will need to access by storing work on the shared drive, T: in the appropriate subject folder. Students will also be able to place files for staff to access on this drive. Periodic cleaning of this drive will take place with files that have not been accessed for a long period of time being deleted, so staff should delete files as soon as they are no longer required; files left on this drive should be a copy. Any files\folders with inappropriate names will be deleted. Photographs of students should not be placed on the T drive.

6. Legal requirements

Users should make themselves aware of the legal requirements when using computerised records. Please refer to the section on Data Protection.

System for reporting security incidents
Any breaches of security should be dealt with immediately and reported to the ICT Systems Manager.

Backing up the system
Full system backups are performed weekly on a Friday to a dedicated backup server using the popular Veritas Backup Exec software; additionally, a full backup is also taken and stored on a Synology NAS device.

Once a month the onsite Senior ICT Technician perform a manual backup of all staff and student's documents to which are backed up to a removal hard drive. To which is then stored away for safe keeping at the end of the month when a replacement hard drive is then added for the following month, a total of 12 months' data is kept in storage.

Software Policy
1. Legal requirements

Only software with sufficient licenses will be installed on the network.

2. Consistent software

The school has adopted Microsoft Office and Google Suite as the main software to be used.

3. Installing new software

Software to be installed on the network is to be installed by the ICT Systems Manager due to the level of access required to install software and the necessity for the ICT Systems Manager to be aware of all software that is accessed on the network.

Data Protection Principles
Staff should ensure they are aware that:

Registered data users must comply with the Data Protection Principles in relation to the personal data they hold. Broadly they state that personal data shall:
- Be obtained and processed fairly and lawfully.
- Be held only for lawful purposes which are described in the register entry.
- Be used or disclosed only for those or compatible purposes.

- Be adequate, relevant and not excessive in relation to the purpose for which they are held.
- Be accurate and, where necessary, kept up to date.
- Be held no longer than is necessary for the purpose for which they are held.
- Be able to allow individuals to access information held about them and where appropriate, correct or erase it.
- Be surrounded by proper security.

The principles also provide for individuals to have access to data held about themselves and, where appropriate, to have the data corrected or deleted.

To enforce compliance with the Principles, the Registrar can serve three types of notice:

- An enforcement notice, requiring the data user to take specified action to comply with the principle. Failure to comply with the notice would be a criminal offence.
- A de-registration notice, cancelling the whole or part of a data user's register entry. It would then be a criminal offence for the data user to continue to treat the personal data subject to the notice as though they were still registered in the same way.
- A transfer prohibition notice, preventing the data user from transferring personal data overseas if the Registrar is satisfied that the transfer is likely to lead to a principle being broken. Failure to comply with the notice would be a criminal offence.

Appendix 7: ICT network and SIMS overview

Usernames, Passwords and Security
All members of staff are issued with:

- Network username and password. (These are also used to access the Intranet and SIMS Learning Gateway from home).
- Automatic login to SIMS (the school management information system) which ensures that the user is automatically signed into SIMS when they log onto the network.
- A username and password for gmail, the school email system. It is expected that members of staff will log into gmail at least twice a day to check their emails. All email correspondence with colleagues and students should be restricted to gmail, as the filtering system protects the user from abuse.

Individual members of staff must ensure that other users, particularly students, do not gain access to their login either by leaving a computer logged in or by sharing a password with another user. Under NO circumstances may students be allowed to use a computer which is logged in as a member of staff. This would give the student access to confidential information in SIMS as well as in the Staff only Q: drive. If a member of staff needs to leave a room in which they are logged onto a computer they should use CTRL + ALT + DEL and lock the computer.
Availability, booking and use of ICT Suites

The following summarises how the ICT suites are timetabled:

- C33, C34 - main teaching rooms of the ICT department, unused periods can be booked.
- B58 – available for advanced timetabling or ad hoc booking.
- E25 – DT ICT suite. Available for booking when not required by DT or ICT.
- Library – ICT suite is used for ASDAN lessons and English library lessons. Available for booking when not required for timetabled sessions.

Booking:
Departments should have identified ICT requirements within the schemes of work. Bookings for the required numbers of sessions should be requested by the end of the summer term for the next academic year. These requests will be accommodated wherever possible. Priority will be given to:

- Controlled assignments where the exam board requires the final work to be computer generated.
- Development work requiring individual student access to specialist subject software on the network.
- Online tests.

Ad hoc bookings are made in the office or the google calendar which also displays availability/usage.

Whether booking in advance or using ad hoc bookings you will be required to provide information about the class, number of students and purpose.

Using ICT Suites:

- No bags and absolutely no food or drink.
- Structured lessons – students still need the structure, expectations, lesson objectives and learning outcomes.
- Students must not be allowed to disconnect equipment.
- Impero is available in all ICT suites, some of the useful features are:
  - monitor student use of the PC
  - restrict use of internet
  - restrict internet sites available
  - restrict software available
  - show your desktop to the students via their desktop whilst also taking control of their PC to gain their attention as you demonstrate what is required or how to use a specific aspect of the software
  - take control of individual or multiple PCs to gain student attention
- Printing – students should not be printing unless you have checked their work, use print preview to ensure no blank pages, ensure name and class is on the work (using headers and footers).

Software Availability and installation

All software on the network is either installed on the central servers or is pushed out to PCs via the servers. It is therefore relatively straightforward for software to be made available on an additional PC or in an additional room. If you have new software that you would like to be added to the network, you should log a request via the ICT Help Centre and place the installation discs and licence documentation in the ICT System Manager's pigeonhole. Original licence documents and installation discs will be held by the ICT Support department in a secure location and a copy of the installation discs will be returned to your Head of Department.

ICT Help Centre

Staff should use the ICT Help Desk faults which is available via the homepage. All technical problems, equipment faults or questions should be logged here. An email response will be received indicating the status of the case. If the case cannot be resolved quickly the response will indicate what will be required and may ask for further information.

Network Restrictions for Students

Some restrictions can be applied to students who misuse computers. When applying these restrictions, they should form part of a sanction and the behaviour incident logged in SIMS. The restrictions which can be applied are as follows.

- Internet blocked at all times – this can only be requested by SLT.
- Network access restricted to certain lessons - this can only be requested by SLT.
- Network access restricted at all times - this can only be requested by SLT.

Appendix 8: West Norfolk Acadamies Trust Bring Your Own Device (BYOD) Acceptable Use Policy (AUP)

What is a Personally Owned Device?
A personally owned device will include, but not be limited to, the following:

iPad, Smartphone, Nook, Kindle or other tablet PC, laptop and netbook computer If a student is unsure if the device is acceptable they should ask a member of the school ICT team before registering the device. The policies outlined in this document are intended to cover all available 'smart' technologies and are not limited to those specifically listed.

Expectations:
The school has set out below the expectations regarding student use of their personally owned devices. All these expectations will apply to students when they are in or around the school. Misuse of a device will result in the device being banned from the network.

The entitlement to use a personal device in school is currently available to students with prior consent from the SENCo only.

To work in line with this policy, students will:

- Only use appropriate technology at the discretion of school staff.
- Use their device for educational purposes only
- Limit their use to appropriate and purposeful educational applications and/or programs on their device.
- Only access appropriate and purposeful educational files on their device.
- Be permitted to access only the school's network through their personal devices, not private networks. Students are not allowed to use their own 3G or 4G service while at school for the transmission of data.
- Be aware that the school is not liable for loss, damage, misuse, or theft of personally owned devices brought to school under any circumstances whatsoever, even if left in locked rooms (eg changing rooms).
- Observe all school internet filters.
- Not connect their devices to the local area network via an Ethernet cable.
- Only access the network using the provided wireless network.
- Not use any device as a cyber-bullying tool or for any other offensive communication.
- Use headphones when listening to audio files such as music on their device so that the volume should be kept at a level which will not disrupt others.

While they are in the classroom, students may only listen to audio files when given express permission by their teachers.

- Follow copyright laws concerning illegal copying of music, games, movies and other protected works.
- Not be allowed to use gaming consoles or gaming devices to connect to the network.
- Be prohibited from taking pictures or digital recordings of staff or students without their prior written permission. The distribution of such media will be taken very seriously.
- Never share usernames and passwords with other students or staff.

Educational Purposes:
Students will use their electronic device for educational purposes only. This may be during a classroom activity, such as researching a topic, using a calculator for mathematical problems, creating maps, note taking, planner/calendar, document creation, or connecting to electronic resources provided by the school.

Students are responsible for their personal device and must check with teaching staff or the ICT team before engaging in particular uses of technology.

Inappropriate communication:
As a school, we recognise that in order for our students to learn and develop to the best of their ability, they need (and deserve) to feel safe. We are very clear that any form of bullying, harassment or abuse is not acceptable and will work with students and parents together to address this whenever it occurs. We are also very aware of the potential for these behaviours to take place on-line. As a school, we recognise that use of IT and personal devices is very much part of 21st Century living. Our policy concerning the use of personal devices in school is really clear and aims to encourage and support the safe and responsible use of technology, with clear consequences in place for any inappropriate use.

Access to the internet is of course '24/7' and we recognise the potential for inappropriate on-line behaviour involving students to take place outside school and school hours. The school will address any inappropriate on-line behaviour involving any of its students, whenever it has an impact on the sense of safety and subsequently learning and development in school of other students. Any questions or concerns should be raised with the SENCo or Designated Safeguarding Lead in the first instance.
Students will refrain from using their device for inappropriate communications. These include but are not limited to the following:
bullying, threatening, obscene, profane, vulgar language and/or images which may cause damage to an individual or the school.

Students will not use their devices for the purposes of harassment, stalking or personal attacks on other students or staff. If a student is instructed to stop sending electronic communications they must do so immediately.

Security:
The School provides content filtering for student access to the Internet. However, inappropriate material may occasionally bypass the filters and be viewed by a student. Students should report the occurrence to their teacher or the ICT team. Students will be held accountable for any deliberate attempt to bypass the LGFL filters and security. All devices must be stowed away when not in use. The School strongly recommends that machines and carry cases are personalised to reduce the risk of loss.

Consequences of Violations:
Using your own device in school is a privilege, not a right. Students who do not follow the expectations for use of personal devices will lose the privilege to utilise personal devices in school for a period of time.

1. First Offence - Verbal warning.
2. Second Offence - Loss of BYOD privileges for a week, with contact home.
3. Third offence - Indefinite loss of BYOD privileges.

The school reserves the right to vary these consequences in the event of a serious breach, particularly if a safeguarding issue is identified.
User protocols:

Users must respect and protect the privacy of others by:
1. Using only assigned accounts.
2. Only viewing, using, or copying passwords, data, or networks to which they are authorised.
3. Refraining from distributing private information about others or themselves.

Users must respect and protect the integrity, availability, and security of all electronic resources by:

1. Observing all Sophos internet filters and posted network security practices.
2. Reporting any security risks or violations they may observe to a teacher or network administrator.
3. Not destroying or damaging data, networks, or other resources which do not belong to them, without clear permission of the owner.
4. Conserving, protecting, and sharing these resources with other users.
5. Notifying a staff member or ICT team member of computer or network malfunctions.

Users must respect and protect the intellectual property of others by:

1. Adhering to copyright laws (not making illegal copies of music, games, or movies).
2. Citing sources when using others' work (not plagiarising).

Users must respect and practice the principles of community by:

1. Communicating only in ways which are kind and respectful.
2. Reporting threatening or discomforting materials to a teacher or ICT team member.
3. Not intentionally accessing, transmitting, copying, or creating material which violates the school's Behaviour Policy (such as messages/content which are pornographic, threatening, rude, discriminatory, or meant to harass).
4. Not intentionally accessing, transmitting, copying, or creating illegal material (such as obscenity, stolen materials, or illegal copies of copyrighted works).
5. Not using the resources to further other acts which are criminal or violate the school's Behaviour Policy.
6. Avoiding spam, chain letters, or other mass unsolicited mailings.
7. Refraining from buying, selling, advertising, or otherwise conducting business, unless approved as a school project.

Users may, if in accordance with the policy above:

1. Design and post web pages and other material from school resources.
2. Communicate electronically via tools such as email, chat, text, or videoconferencing (students require a teacher's permission).
3. Install or download software, in conformity with laws and licenses, (students must be under the supervision of a teacher) for example, NearPod or Evernote/Skitch.
4. Use the resources for any educational purpose

Social, Web Tools and Collaborative Content:

Recognising the benefits which collaboration brings to education, the school may provide students with access to websites or tools to allow communication, collaboration, sharing, and messaging among users. All school rules apply to online behaviour.

Supervision and Monitoring:

- School and network administrators and their authorised employees monitor the use of information technology resources to ensure that uses are secure and in conformity with this policy.
- Administrators reserve the right to examine, use, and disclose any data found on the school's information networks in order to further the health, safety, discipline, or security of any student or other person, or to protect property. They may also use this information in disciplinary actions, and will furnish evidence of crime to law enforcement agencies.
- The school reserves the right to determine which uses constitute acceptable use and to limit access to such uses. The school also reserves the right to limit the time of access.

Technical support and network connections:
Students who cannot access the wireless network or have technical issues with their device should resolve this issue by working with the user manual provided with the device outside the classroom or contact the seller directly. These are not school owned devices, and the school cannot allocate resources to troubleshoot connection issues or faulty devices, beyond reasonable in-house support.

Charging:
Students are responsible for ensuring that devices are charged before they come into the school.

Printing:
We are not currently able to offer direct printing facilities.

West Norfolk Academies Trust
Bring Your Own Device (BYOD) Acceptable Use Policy (AUP)

STUDENT APPLICATION

I wish to apply for BYOD access rights. I confirm receipt of the school policy and agree to abide by its terms and conditions. I understand that access rights may be removed at any time by the school. I will not divulge my log-in details to anyone else and will report any possible breach to the ICT manager.

Name:……………………………………………………Tutor Group: ……………………………….

School: ………………………………………………………………………………………………..

Signature: ………………………………………………………………… Date: …………………