On-Line Safety Policy

Policy reviewed, updated and ratified by the GB:	**Mar 19**
Date of next review:	**Mar 22**

Rationale

The purpose of this policy is to:

- Set out the key principles expected of all members of the school community at Northwood School with respect to the use of IT-based technologies.
- Safeguard and protect the children and staff.
- Assist school staff working with children to work safely and responsibly with the Internet and other IT and communication technologies and to monitor their own standards and practice.
- Set clear expectations of behaviour and/or codes of practice relevant to responsible use of the Internet for educational, personal or recreational use for the whole school community.
- Have clear structures to deal with online abuse such as online bullying [noting that these need to be cross referenced with other school policies].
- Ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- Minimise the risk of misplaced or malicious allegations made against adults who work with students.

The main areas of risk for our school community can be summarised as follows:

Content

- Exposure to inappropriate content
- Lifestyle websites promoting harmful behaviours
- Hate content
- Content validation: how to check authenticity and accuracy of online content

Contact

- Grooming (sexual exploitation, radicalisation etc.)
- Online bullying in all forms
- Social or commercial identity theft, including passwords

Conduct

- Aggressive behaviours (bullying)
- Privacy issues, including disclosure of personal information
- Digital footprint and online reputation
- Health and well-being (amount of time spent online, gambling, body image)
- Sexting
- Copyright (little care or consideration for intellectual property and ownership)

Scope

This policy applies to all members of Northwood School community (including staff, students/students, volunteers, parents/carers, visitors, community users) who have access to and are users of the school's IT systems, both in and out of Northwood School.

Roles and responsibilities

Role	Key Responsibilities
Headteacher	To lead a 'safeguarding' culture, ensuring that online safety is fully integrated with whole school safeguarding. To take overall responsibility for online safety provision To take overall responsibility for data management and information security (SIRO) ensuring school's provision follows best practice in information handling To ensure the school uses appropriate IT systems and services including, filtered Internet Service, e.g. LGfL services To be responsible for ensuring that all staff receive suitable training to carry out their safeguarding and online safety roles To ensure that there is a system in place to monitor and support staff who carry out internal online safety procedures, e.g. network manager To ensure Governors are regularly updated on the nature and effectiveness of the school's arrangements for online safety To ensure the school website includes relevant information
Online Safety Co-ordinator	Must be adequately trained in off-line and online safeguarding, in-line with statutory guidance and relevant Local Safeguarding Children Board (LSCB) guidance Take day to day responsibility for online safety issues and a leading role in establishing and reviewing the school's online safety policy/documents Promote an awareness and commitment to online safety throughout the school community Ensure that online safety education is embedded within the curriculum Liaise with school technical staff where appropriate To communicate regularly with LG To ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident To ensure that online safety incidents are logged as a safeguarding incident Facilitate training and advice for all staff Oversee any student surveys / student feedback on online safety issues Liaise with the Local Authority and relevant agencies
Head of Computer Science	To oversee the delivery of the online safety element of the Computing curriculum
Network Manager and/or technician	To report online safety related issues that come to their attention, to the Online Safety Coordinator

	To manage the school's computer systems, ensuring: ▪ school password policy is strictly adhered to ▪ systems are in place for misuse detection and malicious attack (e.g. keeping virus protection up to date) ▪ access controls/encryption exist to protect personal and sensitive information held on school-owned devices ▪ the school's policy on web filtering is applied and updated on a regular basis That they keep up to date with the school's online safety policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant That the use of school technology and online platforms are regularly monitored and that any misuse/attempted misuse is reported to the online safety co-ordinator/Headteacher To ensure appropriate backup procedures and disaster recovery plans are in place To keep up-to-date documentation of the school's online security and technical procedures To ensure all LGfL services are managed on behalf of the school following data handling procedures as relevant
Data and Information Managers	To ensure that the data they manage is accurate and up-to-date Ensure best practice in information management. i.e. have appropriate access controls in place, that data is used, transferred and deleted in-line with data protection requirements. The school must be registered with Information Commissioner
Teachers	To embed online safety in the curriculum To supervise and guide students carefully when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant) To ensure that students are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws
All staff, volunteers and contractors.	To read, understand, sign and adhere to the school staff Acceptable Use Agreement, and understand any updates annually. The AUA is signed by new staff on induction. To report any suspected misuse or problem to the online safety coordinator To maintain an awareness of current online safety issues and guidance e.g. through CPD To model safe, responsible and professional behaviours in their own use of technology At the end of the period of employment/volunteering to return any equipment or devices loaned by the school. This will include leaving PIN numbers, IDs and passwords to allow devices to be reset, or meeting with line manager and technician on the last day to log in and allow a factory reset.
Students	Read, understand, sign and adhere to the Student Acceptable Use Agreement

	To understand the importance of reporting abuse, misuse or access to inappropriate materials To know what action to take if they or someone they know feels worried or vulnerable when using online technology To understand the importance of adopting safe behaviours and good online safety practice when using digital technologies out of school and realise that the school's online safety policy covers their actions out of school To contribute to any 'student voice' / surveys that gathers information of their online experiences
Parents/carers	To read, understand and promote the school's Student Acceptable Use Agreement with their child/children To consult with the school if they have any concerns about their children's use of technology To support the school in promoting online safety and endorse the Parents' Acceptable Use Agreement which includes the students' use of the Internet and the school's use of photographic and video images

Communication:

The policy will be communicated to staff/students/community in the following ways:

- Policy to be posted on the school website.
- Policy to be part of school induction pack for new staff.
- Regular updates and training on online safety for all staff.
- Acceptable use agreements to be issued to whole school community, on entry to the school.

Handling Incidents:

- The school will take all reasonable precautions to ensure online safety.
- Staff and students are given information about infringements in use and possible sanctions.
- Online Safety Coordinator acts as first point of contact for any incident.
- Any suspected online risk or infringement is reported to Online Safety Coordinator that day
- Any concern about staff misuse is always referred directly to the Headteacher, unless the concern is about the Headteacher in which case the compliant is referred to the Chair of Governors and the LADO (Local Authority's Designated Officer).

Review and Monitoring

- The online safety policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the school
- There is widespread ownership of the policy and it has been agreed by the LG and approved by Governors. All amendments to the school online safety policy will be disseminated to all members of staff and students.

2. Education and Curriculum

Student online safety curriculum

This school:

- Has a clear, progressive online safety education programme as part of the Computing curriculum/PSHCE and other curriculum areas as relevant. This covers a range of skills and behaviours appropriate to their age and experience;
- Plans online use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas;
- Will remind students about their responsibilities through the student Acceptable Use Agreement;
- Ensures staff are aware of their responsibility to model safe and responsible behaviour in their own use of technology, e.g. use of passwords, logging-off, use of content, research skills, copyright;
- Ensures that staff and students understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright/intellectual property rights;
- Ensure students only use school-approved systems and publish within appropriately secure / age-appropriate environments.

Staff and governor training

This school:

- Makes regular training available to staff on online safety issues within the school's CPD program;
- Provides, as part of the induction process, all new staff with information and guidance on the Online Safety Policy and the school's Acceptable Use Agreements.

Parent awareness and training

This school as required:

- Provides induction for parents which includes online safety;
- Runs a rolling programme of online safety advice, guidance and training for parents.

3. Expected Conduct and Incident management

Expected conduct

In this school, all users:

- Are responsible for using the school IT and communication systems in accordance with the relevant Acceptable Use Agreements;
- Understand the significance of misuse or access to inappropriate materials and are aware of the consequences;
- Understand it is essential to reporting abuse, misuse or access to inappropriate materials and know how to do so;
- Understand the importance of adopting good online safety practice when using digital technologies in and out of school;
- Know and understand school policies on the use of mobile and hand held devices;

Staff, volunteers and contractors

- Know to be vigilant in the supervision of children at all times, as far as is reasonable, and uses common-sense strategies in learning resource areas where older students have more flexible access;
- Know to take professional, reasonable precautions when working with students, previewing websites before use; using age-appropriate (student friendly) search engines where more open Internet searching is required with younger students;

Parents/Carers

- Should provide consent for students to use the Internet, as well as other technologies, as part of the Acceptable Use Agreement;

Incident Management

In this school:

- There is strict monitoring and application of the online safety policy and a differentiated and appropriate range of sanctions;
- All members of the school are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the school's escalation processes;
- Support is actively sought from other agencies as needed (i.e. the local authority, LGfL, UK Safer Internet Centre helpline, CEOP, Prevent Officer, Police, IWF) 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 the school;
- 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 students 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 – Police, Internet Watch Foundation and inform the LA.

4. Managing IT and Communication System

Internet access, security (virus protection) and filtering

This school:

- Informs all users that Internet/email use is monitored;
- Has the educational filtered secure broadband connectivity through the LGfL;
- Uses the LGfL filtering system which blocks sites that fall into categories (e.g. adult content, race hate, gaming). All changes to the filtering policy are logged and only available to staff with the approved 'web filtering management' status;
- Uses USO user-level filtering where relevant;
- Ensures network health through use of Sophos anti-virus software (from LGfL);
- Uses DfE, LA or LGfL approved systems including DfE S2S, LGfL USO FX2, Egress secure file/email to send 'protect-level' (sensitive personal) data over the Internet
- Uses encrypted devices or secure remote access where staff need to access 'protect-level' (sensitive personal) data off-site;
- Works in partnership with the LGfL to ensure any concerns about the system are communicated so that systems remain robust and protect students.
- Uses classroom management and safeguarding software including Impero and Securly which captures breaches on the following categories – bullying, child protection, drugs, weapons, self-harm, others.

Network management (user access, backup)

This school:

- Uses individual, audited log-ins for all users;
- Uses guest accounts occasionally for external or short term visitors for temporary access to appropriate services;
- Uses teacher 'remote' management control tools for controlling workstations/viewing users/setting-up applications and Internet web sites, where useful;
- Ensures the Systems Administrator/network manager is up-to-date with LGfL services and policies/requires the Technical Support Provider to be up-to-date with LGfL services and policies;
- Has daily back-up of school data (admin and curriculum);
- Uses secure, 'Cloud' storage for data back-up that conforms to DfE Guidance https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/644845/Cloud-services-software-31.pdf
- Storage of all data within the school will conform to the EU and UK data protection requirements; Storage of data online, will conform to the EU GDPR directive; https://www.eugdpr.org/
  where storage is hosted within the EU.

To ensure the network is used safely, this school:

- Ensures staff read and sign that they have understood the school's Online Safety Policy.
- All students have their own unique username and password which gives them access to the Internet and other services;
- Makes clear that no one should log on as another user and makes clear that students should never be allowed to log-on or use teacher and staff logins;
- Has set-up the network with a shared work area for students and one for staff. Staff and students are shown how to save work and access work from these areas;
- Requires all users to log off when they have finished working or are leaving the computer unattended;
- Ensures all equipment owned by the school and/or connected to the network has up to date virus protection;
- Makes clear that staff are responsible for ensuring that any computer or laptop loaned to them by the school, is used primarily to support their professional responsibilities.
- Makes clear that staff accessing LA systems do so in accordance with any Corporate policies; e.g. Borough email or Intranet; finance system, Personnel system etc.
- Maintains equipment to ensure Health and Safety is followed;
- Ensures that access to the school's network resources from remote locations by staff is audited and restricted and access is only through school/LA approved systems:
- Does not allow any outside Agencies to access our network remotely except where there is a clear professional need;
- Has a clear disaster recovery system in place that includes a secure, remote off site back up of data;
- Ensures that all student level data or personal data sent over the Internet is encrypted or only sent within the approved secure system in our LA or through USO secure file exchange (USO FX); Our wireless network has been secured to industry standard Enterprise security level /appropriate standards suitable for educational use;
- All IT and communications systems installed professionally and regularly reviewed to ensure they meet health and safety standards;

Password policy

- This school makes it clear that staff and students must always keep their passwords private, must not share with others; If a password is compromised the school should be notified immediately.
- All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password(s) private.
- We require staff to use STRONG passwords.
  We require staff using critical systems to use two factor authentication.

E-mail

This school

- Provides staff with an email account for their professional use and makes clear personal email should be through a separate account;
- Uses anonymous or group e-mail addresses, for example info@schoolname.la.sch.uk/head@schoolname.la.sch.uk/or class e-mail addresses.
- Will contact the Police if one of our staff or students receives an e-mail that we consider is particularly disturbing or breaks the law.
- Will ensure that email accounts are maintained and up to date
- Uses a number of LGfL-provided technologies to help protect users and systems in the school, including desktop anti-virus product Sophos and anti-malware/ransomware product Malwarebytes.

Students:

- Students are taught about the online safety and 'netiquette' of using e-mail both in school and at home.

Staff:

- Staff should only use Google e-mail systems on the school system for professional purposes
- Access in school to external personal e-mail accounts may be blocked
- Never use email to transfer staff or student personal data. '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.

School website

- The Headteacher takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained;
- The school website complies with statutory DFE requirements;
- Most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status;
- Photographs published on the web do not have full names attached. We do not use students' names when saving images in the file names or in the tags when publishing to the school website;

Cloud Environments

- Uploading of information on the schools' online learning space is shared between different staff members according to their responsibilities e.g. all class teachers upload information in their class areas;
- Photographs and videos uploaded to the school's online environment will only be accessible by members of the school community;
- In school, students are only able to upload and publish within school approved 'Cloud' systems.

Social networking

Staff, Volunteers and Contractors

- Staff are instructed to always keep professional and private communication separate.

- Teachers are instructed not to run social network spaces for student use on a personal basis or to open up their own spaces to their students, but to use the schools' preferred system for such communications.
- The use of any school approved social networking will adhere to school's communications policy.

School staff will ensure that in private use:

- No reference should be made in social media to students/ parents/carers or school staff;
- School staff should not be online friends with any student. Any exceptions must be approved by the Headteacher.
- They do not engage in online discussion on personal matters relating to members of the school community;
- Personal opinions should not be attributed to the school or local authority and personal opinions must not compromise the professional role of the staff member, nor bring the school into disrepute;
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

  See Social Media Policy for more detail

Students:

- Are taught about social networking, acceptable behaviour and how to report misuse, intimidation or abuse through our online safety curriculum work.
- Students are required to sign and follow our Student Acceptable Use Agreement.

CCTV

- We have CCTV in the school as part of our site surveillance for staff and student safety. The use of CCTV is clearly signposted in the school. We will not reveal any recordings without appropriate permission.
- We may use specialist lesson recording equipment on occasions as a tool to share best teaching practice. We do not reveal any such recordings outside of the staff and will not use for any other purposes.

5. Data security: Management Information System access and Data transfer

Strategic and operational practices

At this school:

- The Headteacher is the Senior Information Risk Officer (SIRO).
- Staff are clear who are the key contact(s) for key school information.
  We ensure staff know who to report any incidents where data protection may have been compromised.

  See The Data Protection Policy for more detail

- All staff are DBS checked and records are held in a single central record

Technical Solutions

- Staff have secure area(s) on the network to store sensitive files
- All servers are in lockable locations and managed by DBS-checked staff
- Details of all school-owned hardware will be recorded in a hardware inventory
- Details of all school-owned software will be recorded in a software inventory
- Disposal of any equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2006 and/or The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007

- Where any protected or restricted data has been held we get a certificate of secure deletion for any server that once contained personal data
- We are using secure file deletion software

6. Equipment and Digital Content

Mobile Devices

- Mobile devices brought into school are entirely at the staff member, students & parents or visitors own risk. The school accepts no responsibility for the loss, theft or damage of any phone or hand held device brought into school
- Mobile devices brought in to school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally-owned mobile devices
- Personal mobile devices will not be used during lessons or formal school time unless as part of an approved and directed curriculum-based activity with consent from linked LG members
- Student personal mobile devices, which are brought into school, must be turned off (not placed on silent) and stored out of sight on arrival at school. They must remain turned off and out of sight until the end of the day
- Staff members may use their phones during school break times
- The school reserves the right to search the content of any mobile devices on the school premises where there is a reasonable suspicion that it may contain illegal or undesirable material, including pornography, violence or bullying. Staff mobiles devices may be searched at any time as part of routine monitoring
- If a student needs to contact his or her parents or carers, they will be allowed to use a school phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office

Storage, Synching and Access

The device is accessed with a school owned account

- The device has a school created account and all apps and file use is in line with this policy. No personal elements may be added to this device
- PIN access to the device must always be known by the network manager

The device is accessed with a personal account

- If personal accounts are used for access to a school owned mobile device, staff must be aware that school use will be synched to their personal cloud, and personal use may become visible in school and in the classroom
- PIN access to the device must always be known by the network manager
- Exit process – when the device is returned the staff member must log in with personal ID so that the device can be Factory Reset and cleared for reuse

Students' use of personal devices

- The School strongly advises that student mobile phones and devices should not be brought into school
- The School accepts that there may be particular circumstances in which a parent wishes their child to have a mobile phone for their own safety
- If a student breaches the school policy, then the device may be confiscated and may be held in a secure place in the school office. Mobile devices will be released to parents or carers in accordance with the school policy
- Phones and devices must not be taken into examinations. Students found in possession of a mobile device during an exam will be reported to the appropriate examining body. This may result in the student's withdrawal from either that examination or all examinations.

Staff use of personal devices (mobile phones, personal cameras, laptops, tablets etc.)

- Staff should not use personally-owned devices, such as mobile phones or cameras, to take photos or videos of students and should only use work-provided equipment for this purpose
- Mobile Phones and personally-owned devices will be switched off or switched to 'silent' mode. Bluetooth communication should be 'hidden' or switched off and mobile phones or personally-owned devices will not be used during teaching periods unless permission has been granted by a member of the Leadership Group in emergency circumstances
- If members of staff have an educational reason to allow children to use mobile phones or a personally-owned device as part of an educational activity, then it will only take place when approved by the Leadership Group
- In an emergency where a staff member doesn't have access to a school-owned device, they should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes
- If a member of staff breaches the school policy, then disciplinary action may be taken

Digital images and video

In this school:

- 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;
- We do not identify students in online photographic materials or include the full names of students in the credits of any published school produced video materials;
- Staff sign the school's Acceptable Use Agreement and this includes a clause on the use of mobile phones/personal equipment for taking pictures of students;
- The school blocks/filter access to social networking sites unless there is a specific approved educational purpose;
- Students are taught about how images can be manipulated in their online safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children as part of their computing scheme of work;
- Students are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information
- Students are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse

This Policy links to the Following Policies and Statements:

- Child Protection Policy
- The Whistleblowing Policy
- Prevent Strategy
- Accessibility Plan
- Equalities Statement & Objectives
- Anti-Bullying Policy
- Data Protection Policy
- Social Media Policy

Appendices

- Acceptable Use Agreement (Staff)

- First Line Information for E-safety Incidents: http://www.digitallyconfident.org/resources/first-line-information
- Radicalisation and Extremism: https://www.gov.uk/government/publications/protecting-children-from-radicalisation-the-prevent-duty
- A6:Data security: Use of IT systems and Data transfer
- Search and Confiscation: https://www.gov.uk/government/publications/searching-screening-and-confiscation

Appendix 1

Acceptable Use Policy for Staff

Networked resources, including Internet access, are potentially available to all students and staff at Northwood School. All users are required to follow the conditions laid down in this policy. Any breach of these conditions may lead to withdrawal of the user's access, monitoring and or retrospective investigation of the users use of services, and in some instances could lead to criminal prosecution. Any breach of the conditions will also be considered a disciplinary matter.

These networked resources are intended for educational purposes, and may only be used for legal activities consistent with the rules of the School. Any expression of a personal view about the School matters in any electronic form of communication must be endorsed to that effect. Any use of the network that would bring the name of the Northwood School into disrepute is not allowed.

The School expects that staff will use new technologies as appropriate within the curriculum and that staff will provide guidance and instruction to learners in the use of such resources. Independent student use of the Internet or the School's Intranet will only be permitted upon receipt of signed permission and agreement

forms as laid out below. All computer systems will be regularly monitored to ensure that they are being used in a responsible fashion.

Personal Responsibility
Access to the networked resources is a privilege, not a right. Users are responsible for their behaviour and communications. Staff and students will be expected to use the resources for the purposes for which they are made available. Users are to take due care with the physical security of hardware they are using. Users will accept personal responsibility for reporting any misuse of the network to the network manager.

Acceptable Use
Users are expected to utilise the network systems in a responsible manner. It is not possible to set hard and fast rules about what is and what is not acceptable but the following list provides some guidelines on the matter:

- Network Etiquette and Privacy - Users are expected to abide by the rules of network etiquette. These rules include, but are not limited to, the following:

    - Be polite – never send or encourage others to send abusive messages.
    - Use appropriate language – users should remember that they are representatives of the School on a global public system. Illegal activities of any kind are strictly forbidden.
    - Do not use language that could be calculated to incite hatred against any ethnic, religious or other minority group.
    - Privacy – do not reveal any personal information (e.g. home address, telephone number) about yourself or other users. Do not trespass into other users' files or folders.
    - Password – do not reveal your password to anyone. If you think someone has learned your password, then contact the School's network manager.
    - Electronic mail – Is not guaranteed to be private. Messages relating to or in support of illegal activities will be reported to the authorities. Do not send anonymous messages.
    - Disruptions – do not use the network in any way that would disrupt use of the network by others.

- Staff finding unsuitable websites through the School's network should report the web address to the network manager.
- Do not introduce floppy disks or "pen drives" into the network without having them checked for viruses.
- Do not attempt to visit websites that might be considered inappropriate. Such sites would include those relating to illegal activity. All sites visited leave evidence in the School network if not on the computer. Downloading some material is illegal and the police or other authorities may be called to investigate such use.
- Unapproved system utilities and executable files will not be allowed in learners' work areas or attached to e-mail.
- Files held on the School's network will be regularly checked by the network manager.
- It is the responsibility of the User (where appropriate) to take all reasonable steps to ensure compliance with the conditions set out in this Policy document, and to ensure that unacceptable use of the Internet/Intranet does not occur.

Unacceptable Use
Examples of unacceptable use include but are not limited to the following:
- Users must login with their own user ID and password and must not share this information with other users. They must also log off after their session has finished.
- Users finding machines logged on under other users username should log off the machine whether they intend to use it or not.

- Accessing or creating, transmitting, displaying or publishing any material (e.g. images, sounds or data) that is likely to cause offence, inconvenience or needless anxiety. (The School has filters in place to block e-mails containing language that is or may be deemed to be offensive.) This also includes creating or uploading images of students unless the School's parental consent pro-forma gives permission to do so.
- Accessing or creating, transmitting or publishing any defamatory material.
- Receiving, sending or publishing material that violates copyright law. This includes through Video Conferencing and Web Broadcasting.
- Receiving, sending or publishing material that violates Data Protection Act or breaching the security this act requires for personal data.
- Transmitting unsolicited material to other users (including those on other networks).
- Unauthorised access to data and resources on the School network system or other systems.
- User action that would cause corruption or destruction of other users' data, or violate the privacy of other users, or intentionally waste time or resources on the network or elsewhere.

Additional guidelines

- Users must comply with the acceptable use policy of any other networks that they access.
- Users must not download software without approval from the network manager.
- It is the responsibility of all staff to regularly remind all learners of expected behaviour when using the School network.
- Displays should be prominent around the School to remind learners of expected behaviour and responsibilities information on cyber bullying, including access to help available online.
  This document is to be reviewed on a regular basis.

Services

There will be no warranties of any kind, whether expressed or implied, for the network service offered by the School. The School will not be responsible for any damages suffered while on the system. These damages include loss of data as a result of delays, non-deliveries, or service interruptions caused by the system or your errors or omissions. Use of any information obtained via the network is at your own risk.

Network Security

Users are expected to inform the network manager immediately if a security problem is identified. Do not demonstrate this problem to other users. Users must always login to the School network with their own user id and password, where applicable, and must not share this information with other users. Users identified as a security risk will be denied access to the network, in exceptional cases this may become permanent and police may become involved.

Physical Security

Staff users are expected to ensure that portable ICT equipment such as laptops, digital still and video cameras are securely locked away when they are not being used. Items that need to be left over breaks and lunchtimes for example will need to be physically protected by locks and or alarms.

Wilful Damage

Any malicious attempt to harm or destroy any equipment or data of another user or network connected to the School system will result in loss of access, disciplinary action and, if appropriate, legal referral. This includes the creation or uploading of computer viruses. The use of software from unauthorised sources is prohibited.

Media Publications

Written permission from parents or carers will be obtained before photographs of students are published. Named images of students will only be published with the separate written consent of their parents or carers.

Publishing includes, but is not limited to:

- Northwood School web sites,
- Web broadcasting,
- TV presentations,
- Newspapers.

I ……agree to abide by the above terms of the Northwood School

Acceptable Use policy.

Signed:…… ……

Date:……