Higham Lane School
Helping Learners Succeed

Online Safety and ICT Acceptable Use Policy

Policy Number	**22**
Approval Date	**January 2021**
Review Date	**January 2025**
Governors' Sub-Committee	**Curriculum and Standards**
Statutory Policy	**No**

Signed: David Buckle **Chair of Governors** Date: **Jan 2021**

Contents

1. Introduction

ICT in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

Information and Communications Technology covers a wide range of resources including; webbased and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Apps
- Email, Instant Messaging and chat rooms
- Social Media, including Facebook, Twitter and Snapchat
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices including tablets and gaming devices
- Online Games
- Learning Platforms and Virtual Learning Environments
- Blogs and Wikis
- Podcasting, Video sharing and Downloading
- On demand TV and video, movies and radio / Smart TVs

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies and that some have minimum age requirements (13 years in most cases).

At Higham Lane School, we understand the responsibility to educate our students on online safety issues including safeguarding, radicalisation, extremism and protecting their personal data; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Schools hold personal data on learners, staff and others to help them conduct their day-to-day activities. Some of this information is sensitive and could be used by another person or criminal organisation to cause harm or distress to an individual. The loss of personal information can result in media coverage, and potentially damage the reputation of the school. This can make it more difficult for your school to use technology to benefit learners. Schools must be mindful to protect personal data to comply with GDPR regulations as set out under the Data Protection Act 2018.

Everybody in the school community has a shared responsibility to secure any sensitive information used in their day to day professional duties and even staff not directly involved in data handling should be made aware of the risks and threats and how to minimise them.

Both this policy and the Acceptable Use Agreement (for all staff, governors, regular visitors [for regulated activities] and students) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, mobile devices, webcams, whiteboards, voting systems, digital video equipment, etc.); and technologies owned by students and staff, but brought onto school premises (such as laptops, mobile phones and other mobile devices).

2. Monitoring

Authorised ICT staff may inspect any ICT equipment owned or leased by the school at any time without prior notice. If you are in doubt as to whether the individual requesting such access is authorised to do so, please ask for their identification badge and contact their department. Any ICT authorised staff member will be happy to comply with this request.

ICT authorised staff may monitor, intercept, access, inspect, record and disclose telephone calls, emails, instant messaging, internet/intranet use and any other electronic communications (data, voice, video or image) involving its employees or contractors, without consent, to the extent permitted by law. This may be to confirm or obtain school business related information; to confirm or investigate compliance with school policies, standards and procedures; to ensure the effective operation of school ICT; for quality control or training purposes; to comply with a Subject Access Request and GDPR regulations more generally under the Data Protection Act 2018 or to prevent or detect crime.

ICT authorised staff may, without prior notice, access the email or voicemail account where applicable, of someone who is absent in order to deal with any business-related issues retained on that account.

All monitoring, surveillance or investigative activities are conducted by ICT authorised staff and comply with the Data Protection Act 2018, the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000 (RIPA) and the Lawful Business Practice Regulations 2000.

Please note that personal communications using School ICT may be unavoidably included in any business communications that are monitored, intercepted and/or recorded by the School's ICT monitoring software (see Appendix A).

3. Breaches

A breach or suspected breach of policy by a school employee, contractor or student may result in the temporary or permanent withdrawal of school ICT hardware, software or services from the offending individual. Breaches to personal data must be reported to the Information Commissioner's Office (ICO) within 72 hours (reference Data Protection Policy).

For staff any policy breach is grounds for disciplinary action in accordance with the school Disciplinary Procedure or, for Support Staff, in their Probationary Period as stated.

Policy breaches may also lead to criminal or civil proceedings. The ICO's powers to issue monetary penalties came into force on 25 May 2018, allowing the Information Commissioner's office to serve notices requiring organisations to pay up to £18 million for serious breaches of the Data Protection Act.

The ICO has both investigative and corrective powers including but exclusive to:

- Carry out investigations – data protection audits;
- Access all personal data and any premises and processing equipment from controller/processor;

- Issue to warnings to controller/processor if intended processing operations likely to infringe GDPR;
- Issue reprimands where processing has infringed GDPR;
- Order processing operations are brought into compliance;
- Order rectification or erasure and impose a fine or withdraw certification;
- Limit or ban processing temporarily or indefinitely.

Incident Reporting

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the school's relevant responsible person. Additionally, all security breaches, lost/stolen equipment or data virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to the relevant responsible person. The relevant responsible individuals in the school are as follows: Miss. K Tomlinson, Senior ICT Technician and Data Protection Mr. I Naisbitt, Assistant Headteacher/Designated Data Protection Officer (DPPL)

Please refer to the relevant section on Incident Reporting, Online Safety Log & Infringements.

4. Staff Professional Responsibilities

When using any form of ICT, including the Internet, in school and outside school, for your own protection we advise that you:

- Ensure all electronic communication with students, parents, carers, staff and others is compatible with your professional role and in line with school policies.
- Do not talk about your professional role in any capacity when using social media such as Facebook, Twitter and YouTube.
- Do not put online any text, image, sound or video that could upset or offend any member of the whole school community or be incompatible with your professional role.
- Use school ICT systems and resources for all school business. This includes your school email address, school mobile phone and school video camera.
- Do not give out your own personal details, such as mobile phone number, personal e-mail address or social network details to students, parents, carers and others.
- Do not disclose any passwords and ensure that personal data (such as data held on MIS software) is kept secure and used appropriately.
- Only take images of students and/ or staff for professional purposes, in accordance with school policy (Data Protection Policy) and with the knowledge of SLT.
- Do not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Ensure that your online activity, both in school and outside school, will not bring the School or your professional role into disrepute.
- You have a duty to report any online safety incident which may impact on you, your professionalism or the School.

5. Computer Viruses

- HLS provide and encourage the use of remote desktops to avoid the need for removable storage devices.

- If you suspect there may be a virus on any school ICT equipment, stop using the equipment, turn the device off and place the following notice on the computer “Not in use”. Thereafter contact the school’s ICT technician immediately.
- The School has virus software installed on school devices. Staff are advised to use the scan feature when opening/downloading any files from unknown systems.

6. Data Security

Data Protection: key responsibilities for School Heads and Governors

Security

- The school gives relevant staff access to its Management Information System, with a unique username and password.
- It is the responsibility of everyone to keep passwords secure.
- Staff are aware of their responsibility when accessing school data.
- Staff have been issued with the relevant guidance documents and the Policy for ICT Acceptable Use.
- Staff keep all school related data secure. This includes all personal, sensitive, confidential or classified data.
- Staff should avoid leaving any portable or mobile ICT equipment or removable storage media in unattended vehicles.
- Staff should always carry portable and mobile ICT equipment or removable media as hand luggage, and keep it under your control at all times.
- It is the responsibility of individual staff to ensure the security of any personal or sensitive information contained in documents faxed, copied, scanned or printed. This is particularly important when shared copiers (multi-function print, fax, scan and copiers) are used. This aligns to policy directives as set out in the School’s Data Protection Policy.
- Anyone sending a confidential or sensitive email or fax should notify the recipient before it is sent.

7. Relevant Responsible Persons

A member of the School’s senior leadership team, Mr I Naisbitt, Assistant Headteacher should be familiar with information risks and the school’s response. Previously called a Senior Information Risk Officer (SIRO), who has the following responsibilities:

- They lead on the information risk policy and risk assessment.
- They advise school staff on appropriate use of school technology.

8. Email

8.1 Managing email

- Where appropriate and relevant, the school gives all staff, students and governors their own email account to use for all school business as a work based tool This is to protect staff, minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed.
- The school can provide access to school email accounts for others as and when required – for educational purposes.
- Staff & governors should use their school email for all professional communication.
- It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary email

histories can be traced. The school email account should be the account that is used for all school business.

- Under no circumstances should staff contact students, parents/carers or conduct any school business using personal email addresses. Nor should staff contact students and parents/carers using their school issued email address.
- The school uses Iris Reach in order to send/receive email communication with parents/carers. The management and application of Iris Reach by staff should adhere to the same policy expectations as all other forms of email communication as set out within this policy.
- The school requires a standard disclaimer to be attached to all email correspondence, stating that… *"Disclaimer. This email is intended for the named addressee(s) only and may contain confidential, sensitive or personal information and should be handled accordingly. If you have received this email in error please notify the sender and delete the email and any attachments. Any views or opinions presented are solely those of the author and do not necessarily reflect those of Higham Lane School. Please don't print this email unless you really need to".*
- All emails should be written and checked carefully before sending, in the same way as a letter written on school headed paper.
- Staff sending emails of a confidential nature, e.g. matters pertaining to safeguarding and child protection, are advised to cc. the Headteacher, designated safeguarding lead, line manager or designated line manager.
- Students may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes.
- Emails created or received as part of your school job will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000/Data Protection 2018. You must therefore actively manage your email account as follows:
  - Delete all emails of short-term value
  - Organise email into folders and carry out frequent house-keeping on all folders and archives
  - Composition of emails must be, at all times, professional in tone and manner
  - Staff must inform the School's ICT technicians if they receive an offensive or 'spam' email.

  The School's ICT technicians will in forward incidents of offensive emails onto School's Online Safety Coordinator.
- However you access your school email (whether directly, through webmail when away from the office or on non-school hardware) all the school email policies apply.

8.2 Sending emails

- Refer to the School's email protocol on when and how to send emails – see Appendix E.
- If sending emails containing personal, confidential, classified or financially sensitive data to external third parties or agencies, refer to the Section Emailing Personal or Confidential Information.
- Use only the School's email account (contactus@highamlaneschool.co.uk) when communicating with parents/carers. Staff are advised not to use their own school email account.
- Keep the number and relevance of email recipients, particularly those being copied, to the minimum necessary and appropriate.
- Do not send or forward attachments unnecessarily. Whenever possible, send the location path to the shared drive rather than sending attachments.
- School email is not to be used for personal advertising.

8.3 Receiving emails

- Check your email regularly.
- Activate your ‘out-of-office’ notification when away for extended periods.
- Never open attachments from an untrusted source; consult the School’s ICT technicians.
- Do not use the email systems to store attachments. Detach and save business related work to the appropriate shared drive/folder.
- The automatic forwarding and deletion of emails is not allowed.

8.4 Emailing Personal or Confidential Information

Where your conclusion is that email must be used to transmit such data:

- Do not send the information to any person whose details you have been unable to separately verify (usually by phone)
- Do not identify such information in the subject line of any email
- Request confirmation of safe receipt

9. Online Safety (formerly E-Safety)

Online Safety - Roles and Responsibilities

As online safety is an important aspect of strategic leadership within the school, the Head and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named Whole School ICT coordinator (Online Safety Coordinator) in this school is Mr Tim Anstey. All members of the school community have been made aware of who holds this post. It is the role of the Online Safety Coordinator to keep abreast of current issues and guidance.

Senior Leadership and governors are updated by the Online Safety Coordinator and all governors have an understanding of the issues and strategies at our school in relation to local and national guidelines and advice.

This policy, supported by the school’s acceptable use agreements for staff, governors, visitors and students, is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: child protection, health and safety, data protection, home–school agreements, and behaviour (including the anti-bullying) policy and CPHSE.

Online Safety in the Curriculum

ICT and online resources are increasingly used across the curriculum. It is essential for online safety guidance to be given to the students on a regular and meaningful basis. Online Safety is embedded within our curriculum and we continually look for new opportunities to promote online safety.

- The school has a framework for teaching internet skills in Computer Science lessons in Key Stage 3.
- Educating students about the online risks that they may encounter outside school is done informally when opportunities arise and as part of Computer Science, Personal Development and within tutor time.
- Students are aware of the relevant legislation when using the internet such as GDPR which may limit what they want to do but also serves to protect them.

- Students are taught about copyright, respecting other people's information, safe use of images and other important areas through discussion, modeling and appropriate activities.
- Students are aware of the impact of Cyberbullying and know how to seek help if they are affected by any form of online bullying. Students are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/ carer, teacher/ trusted staff member, or an organisation such as Childline or the 'CEOP report abuse' button.
- Students are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the ICT/Computing curriculum.

Online safety when Remote Learning

The aim is to teach the curriculum in a way so that learning from home replicates the school experience as best it can in remote circumstances. All other school policies will be followed and replicated, whether students are learning from school or from home. We accept there may be times when this cannot be adhered to completely due to for example issues with technology (school and/or home) or by acknowledging that all students' home circumstances are different – some for example may struggle more with keeping up with work set via home learning. When staff are required to work from home in order to deliver education, Higham Lane School shall:

- Provide staff with a secure, school registered device to work from.
- Ensure staff are briefed and familiar with the school's remote working policy.
- Ensure all staff are up to date with data protection training.

When implementing a platform where students are required to engage in online activities, Higham Lane School will:

- Ensure parents are informed of the type of work children are being asked to do.
- Provide information on who is likely to engage with pupils online in order to deliver online teaching.
- Share information and guidance with parents to ensure they are able to effectively monitor their children's safety online.
- Review settings to ensure they are set to the most secure and practical format that is possible.
- Review privacy settings of all platforms used for online teaching (e.g. GSuite, Google Classroom) to ensure children are not placed at risk.
- If uploading information to an open cloud-based system, we will ensure no personal information that identifies individuals is included.
- Take all reasonable steps to ensure that risks of harm to children through inappropriate access via online portals are reduced as far as possible.
- Continuously liaise with our safeguarding team to ensure we are following all relevant safeguarding guidance.

Student access to technology/laptops/smartphones

The school has sought to support all students who do not have sufficient access to technology at home via regular surveys and through providing laptops and internet access where we have been able to. The result is that:

- School laptops will be loaned to students for the duration of self-isolation so that they're able to fully access the curriculum.
- Students who do not have access to the internet, in whatever form, will be provided with a pre-paid 4G wireless dongle for the duration of self-isolation. This applies to a very small minority of students.

Online Safety Skills Development for Staff

- Our staff receive regular information and training on online safety and how they can promote the 'Stay Safe' online messages in the form of staff briefings and INSET training.
- Details of the ongoing staff training programme can be found on the School's virtual learning environment (VLE), namely SharePoint.
- New staff receive information on the school's acceptable use policy as part of their induction
- All staff have been made aware of their individual responsibilities relating to the safeguarding of children within the context of online safety and know what to do in the event of misuse of technology by any member of the school community.
- All staff are encouraged to incorporate online safety activities and awareness within their curriculum areas and ensure they are adequately informed with up-to-date areas of concern.
- This will be led by Mr Tim Anstey, Whole-school ICT and Online Safety Coordinator.

Managing the School Online Safety Messages

- We endeavour to embed online safety messages across the curriculum whenever the internet and/or related technologies are used.
- The online safety policy will be introduced to the students at the start of each school year and an acceptable use agreement signed by Parent/ Carer.
- Online Safety posters will be prominently displayed.
- The key online safety advice will be promoted widely through school displays, newsletters, class activities and so on.
- We participate in Safer Internet Day every February.
- Online Safety key messages and information will be freely available to all stakeholders via the School's website. This will be actively promoted at all times.

10. Incident Reporting, Online Safety Incident Log & Infringements

Incident Reporting

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the school's relevant responsible person or Online Safety Coordinator. Additionally, all security breaches, lost/stolen equipment or data, virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to the senior ICT technician.

Online Safety Incident Form

Keeping a record of online safety incidents can identify trends or specific concerns. A record of incidents reported using the online safety Incident Form will be maintained by the School's Whole School Coordinator (Online Safety Coordinator). Any safeguarding issues arising from online safety incidents must be passed to the Senior DSL (See Appendix F).

Misuse and Infringements

Complaints

Complaints and/ or issues relating to online safety should be made to the Online Safety Coordinator, Assistant Headteacher responsible for E-learning or Headteacher.

Inappropriate Material

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the Online Safety Coordinator.

- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the relevant responsible person, and an investigation by the Headteacher and Mr. I Naisbitt, Assistant Headteacher. Depending on the seriousness of the offence, sanctions could include immediate suspension, possibly leading to dismissal and involvement of police for very serious offences.
- Users are made aware of sanctions relating to the misuse or misconduct by following the appropriate conditions as set out within the School's Behaviour Policy.

11. Internet Access

The internet is an open worldwide communication medium, available to everyone, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people. All internet use is logged and the logs are randomly but regularly monitored. Whenever any inappropriate use is detected it will be followed up.

Managing the Internet

- The school provides students with supervised access to Internet resources (where reasonable) through the school's fixed and Wi-Fi internet connectivity.
- Staff will preview any recommended sites, online services, software and apps before use.
- Searching for images through open search engines is discouraged when working with students.
- If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents will be advised to supervise any further research.
- All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources.
- All users must observe copyright of materials from electronic resources.

Internet Use

- You must not post personal, sensitive, confidential or classified information or disseminate such information in any way that may compromise the intended restricted audience.
- Do not reveal names of colleagues, students, others or any other confidential information acquired through your job on any social networking site or other online application.
- On-line gambling or gaming is not allowed.
- It is at the Headteacher's discretion as to what internet activities are permissible for staff and students and how this is disseminated.

Infrastructure

- Schools subscribing to the Smoothwall web filtering service have the benefit of monitored web activity.
- Higham Lane School is aware of its responsibility when monitoring staff communication under current legislation and takes into account; Data Protection Act 2018, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Regulation of Investigatory Powers Act 2000, Human Rights Act 1998.
- Staff and students are aware that school based email and internet activity can be monitored and explored further if required.
- The school does not allow students access to internet logs.
- The school uses Netsupport management control tools for controlling and monitoring workstations.

- If staff or students discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to the Online Safety Coordinator or teacher as appropriate.
- It is the responsibility of the school, by delegation to the ICT technicians, to ensure that anti-virus protection is installed and kept up-to-date on all school machines.
- Students and staff are not permitted to download programs or files on school based technologies without seeking prior permission from the senior ICT technician.
- If there are any issues related to viruses, the ICT technicians should be informed.

12. Managing Other Online Technologies

Online technologies, including social networking sites, if used responsibly both outside and within an educational context can provide easy to use, creative, collaborative and free facilities. However it is important to recognise that there are issues regarding the appropriateness of some content, contact, culture and commercialism. To this end, we encourage our students to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.

Where relevant, the school endeavours to deny access to social networking and online games websites to students within school.

- All students are advised to be cautious about the information given by others on such websites, for example users not being who they say they are.
- Through external speakers such as the Police, students are taught to avoid placing images of themselves (or details within images that could give background details) on such websites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online.
- Students are always reminded to avoid giving out personal details on websites which may identify them or where they are (full name, address, mobile/ home phone numbers, school details, IM/ email address, specific hobbies/ interests).
- Our students are advised to set and maintain their online profiles to maximum privacy and deny access to unknown individuals.
- Students are encouraged to be wary about publishing specific and detailed private thoughts and information online.
- Our students are asked to report any incidents of Cyberbullying to the school.
- Staff may only create social media accounts, blogs, wikis or other online areas in order to communicate with students using the school learning platform or other systems approved by Mr. I Naisbitt, Assistant Headteacher or by the Headteacher.
- Services such as Facebook, Instagram and Snapchat have a 13+ age rating which should not be ignored http://www.coppa.org/comply.htm

13. Parental Involvement

It is essential for parents/carers to be fully involved with promoting online safety both in and outside of school and to be aware of their responsibilities. We regularly consult and discuss online safety with parents/ carers and seek to promote a wide understanding of the benefits of new technologies, together with the associated risks.

- Parents/carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to the school

- Parents/carers are required to make a decision as to whether they consent to images of their child being taken and used in the public domain (e.g., on school website) to comply with GDPR – Data Protection Act 2018.
- Parents/carers are expected to sign a Home School agreement in the student organizer containing the following statement:

  - □ I/we will support the school approach to online safety and not upload or add any text, image, sound or videos that could upset or offend any member of the school community, or bring the school name into disrepute.
  - □ I/we will ensure that my/our online activity would not cause the school, staff, students or others distress or bring the school community into disrepute.
  - □ I/we will support the school's policy and help prevent my/our child/children from signing up to services such as Facebook, Instagram, Snapchat and YouTube (edit/add services of particular concern here) whilst they are underage (13+ years in most cases).
  - □ I/we will close online accounts if I/we/teachers find that these accounts are active for our underage child/children.

- The school disseminates information to parents relating to online safety where appropriate in the form of;

  - Information evenings
  - Parent Forum
  - My Ed communication app
  - School website information
  - HLS Express

14. Passwords and Password Security

Passwords

- Always use your own personal passwords.
- Make sure you enter your personal passwords each time you logon. Do not include passwords in any automated logon procedures.
- Staff should change temporary passwords at first logon.
- Change passwords whenever there is any indication of possible system or password compromise.
- Do not record passwords or encryption keys on paper or in an unprotected file.
- Only disclose your personal password to authorised ICT support staff when necessary, and never to anyone else. Ensure that all personal passwords that have been disclosed are changed once the requirement is finished.
- Never tell a child or colleague your password.
- If you aware of a breach of security with your password or account inform the senior ICT technician immediately.
- Passwords must contain a minimum of six characters and be difficult to guess.
- Passwords should contain a mixture of upper and lowercase letters, numbers and symbols.
- User ID and passwords for staff and students who have left the school are removed from the system within one day of leaving.

If you think your password may have been compromised or someone else has become aware of your password report this to your ICT support team.

Password Security

Password security is essential for staff, particularly as they are able to access and use personal data. Staff are expected to have secure passwords which are not shared with anyone. The students are expected to keep their passwords private and not to share with others, particularly their friends. Staff and students are regularly reminded of the need for password security.

- All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's Online Safety and ICT Acceptable Use Policy.
- Users are provided with an individual network, email, and Management Information System log-in username. They are also expected to use a personal password and keep it private.
- Students are not permitted to deliberately access online materials or files on the school network or local storage devices of their peers, teachers or others.
- Staff are aware of their individual responsibilities to protect the security and confidentiality of the school networks, and MIS systems, including ensuring that passwords are not shared and are changed periodically. Individual staff users must also make sure that workstations are not left unattended and are locked. The automatic screen lock for the school network is 30 minutes.
- In our school, all ICT password policies are the responsibility of the senior ICT technician and all staff and students are expected to comply with the policies at all times.

15. GDPR – Data Protection Compliance

- Ensure that any school information (personal data) accessed from your own PC is kept secure and is not removed from the school network.
- Ensure you lock your screen before moving away from your computer during your normal working day to prevent unauthorised access.
- Ensure the accuracy of any personal or sensitive information you disclose or share with others and only share personal or sensitive information that is absolutely necessary – remember, do they require this information and in what format?
- Ensure that personal, sensitive, confidential or classified information is not disclosed to any unauthorised person.
- Ensure the security of any personal or sensitive information contained in documents you email, fax, copy, scan or print. This is particularly important when shared copiers (multifunction print, fax, scan and copiers) are used. Personal information contained in an email must be sent as a password protected attachment.
- Only download personal data from systems if expressly authorised to do so by the School's Designated Data Protection Lead or the Headteacher.
- You must not post on the internet personal or sensitive information, or disseminate such information in any way that may compromise its intended restricted audience.
- Keep your screen display out of direct view of any third parties when you are accessing personal, sensitive, confidential or classified information.
- Ensure hard copies of data are securely stored and disposed of after use in accordance with the document labelling.
- Source: Data Protection Policy.

Storing/Transferring Personal or Sensitive Information Using Removable Media

- By using the School's remote desktop facility there should not be a need to use removable media on a regular basis.
- Encrypted removable storage devices are the only allowed storage device permitted to access the school's network. There's strict access to who can copy data off as sanctioned by the senior ICT technician and Mr I Naisbitt, Assistant Headteacher.

- Securely dispose of removable media that may hold personal data.
- Ensure hard drives from machines no longer in service are removed and stored securely or wiped clean.

16. Remote Desktop Access

- You are responsible for all activity via your remote desktop access facility.
- Only use equipment with an appropriate level of security for remote access.
- To prevent unauthorised access to school systems, keep all logon IDs confidential and do not disclose them to anyone.
- Avoid writing down or otherwise recording any network access information. Any such information that is written down must be kept in a secure place and disguised so that no other person will be able to identify what it is.
- Protect school information and data at all times. Take particular care when access is from a non-school environment.

17. Safe Use of Images

Taking of Images and Film

Digital images are easy to capture, reproduce and publish and, therefore, misuse. We must remember that it is not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness. This complies with GDPR regulations (Data Protection Act 2018). Please refer to the School's Data Protection Policy.

- With the written consent of parents/carers (on behalf of students) and staff, the school permits the appropriate taking of images by staff and students with school equipment.
- Parents/carers must sign the school's GDPR consent form to give their consent (opt in) to the taking of images by staff and students with school equipment. The School in turn will keep an official record of consent given by parents/carers on the School's MIS.
- Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of students, this includes when on school/field trips, unless with the express permission of the School's Designated Data Protection Lead or the Headteacher (images can be taken provided they are transferred immediately and solely to the school's network and deleted from the staff device).
- Students are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of students, staff and others without advance permission from the Headteacher.
- The School will check the School's MIS to check which students and staff have permission before any image can be uploaded for publication.

Consent of Adults Who Work at the School

- Consent to use images of all staff who work at the school is sought on induction and a copy is located in the personnel file

Publishing Student's Images and Work

On a child's entry to the school, all parents/carers will be asked to give their consent to use their child's work/photos in the following ways:

- On the school web site.

- In the school prospectus and other printed publications that the school may produce for promotional purposes.
- Recorded/ transmitted on a video or webcam.
- In display material that may be used in the school's communal areas.
- In display material that may be used in external areas, i.e. exhibition promoting the school.
- General media appearances, e.g. local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically).

This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue, e.g. divorce of parents, custody issues, etc.

Parents or carers may withdraw permission, in writing, at any time. Consent must also be given in writing and will be kept on record by the school.

Students' names will not be published alongside their image and vice versa. Email and postal addresses of students will not be published. Students' full names will not be published. Before posting student work on the Internet, a check needs to be made to ensure that permission has been given for work to be displayed.

Only Mr N Kalair (ICT technician), Miss K Tomlinson (senior ICT technician), Mrs J Woodall (resources manager) and Mr. I Naisbitt, Assistant Headteacher have authority to upload to the internet.

Storage of Images

- Images/ films of children are stored securely on the school's network.
- Students and staff are not permitted to use personal portable media for storage of images (e.g. USB sticks) without the express permission of Mr. I Naisbitt, Assistant Headteacher.
- Rights of access to this material are restricted to the teaching staff and students within the confines of the school network or other online school resource.
- K Tomlinson (senior ICT Technician) has the responsibility of deleting the images when they are no longer required, or then the student has left the school.

Webcams and CCTV

- The school uses CCTV for security and safety. The only people with access to view CCTV footage are the ICT technicians, student services, reception, Ben Elliott (Director of Corporate Services) and the estates team. Only the ICT technicians and the senior caretaker have access to view and extract CCTV footage, Notification of camera use is displayed at the front of the school. Please refer to the hyperlink below for further guidance https://ico.org.uk/media/fororganisations/documents/1542/cctv-code-of-practice.pdf and the School's CCTV Policy.
- We do not use publicly accessible webcams in school.
- Webcams will not be used for broadcast on the internet without prior parental consent.
- Misuse of the webcam by any member of the school community will result in sanctions (as listed under the 'inappropriate materials' section of this document).
- Webcams include any camera on an electronic device which is capable of producing video. School policy should be followed regarding the use of such personal devices.

Video Conferencing (MS Teams etc.)

- Consent is sought from parents and carers if their child is involved in video conferences with end-points outside of the school.

- All students are supervised by a member of staff when video conferencing.
- The school keeps a record of video conferences, including date, time and participants.
- Approval from the Headteacher is sought prior to all video conferences within school to end-points beyond the school.
- No part of any video conference is recorded in any medium without the written consent of those taking part.

Additional points to consider:

- Participants in conferences offered by 3rd party organisations may not be DBS checked.
- Conference supervisors need to be familiar with how to use the video conferencing equipment, particularly how to end a call if at any point any person taking part becomes unhappy with the content of the conference.

18. School ICT Equipment & Mobile ICT Equipment

School ICT Equipment

- As a user of the school ICT equipment, you are responsible for your activity.
- It is recommended that the school logs ICT equipment issued to staff and record serial numbers as part of the school's inventory.
- Do not allow your visitors to plug their ICT hardware into the school network points (unless special provision has been made). They should be directed to the wireless ICT facilities if available.
- Ensure that all ICT equipment that you use is kept physically secure.
- Do not attempt unauthorised access or make unauthorised modifications to computer equipment, programs, files or data. This is an offence under the Computer Misuse Act 1990.
- It is imperative that you save your data on a frequent basis to the school's network. You are responsible for the backup and restoration of any of your data that is not held on the school's network.
- Personal or sensitive data should not be stored on the local drives of desktop PC, laptop, USB memory stick or other portable device.
- All school issued laptops are encrypted.

  It is recommended that a time locking screensaver is applied to all machines. Any device accessing personal data must have a locking screensaver as must any user profiles.
- Privately owned ICT equipment should not be used on a school network, apart from internet access which must be approved by the senior ICT technician.
- On termination of employment, resignation or transfer, return all ICT equipment to your Manager. You must also provide details of all your system logons so that they can be disabled.
- It is your responsibility to ensure that any information accessed from your own PC or removable media equipment is kept secure, and that no personal, sensitive, confidential or classified information is disclosed to any unauthorised person.
- All ICT equipment allocated to staff must be authorised by the Assistant Headteacher responsible for e-learning. ICT technicians are responsible for:
  - maintaining control of the allocation and transfer back into school ready for reissue.
  - recovering and returning equipment when no longer needed
- All redundant ICT equipment is disposed of in accordance with Waste Electrical and Electronic Equipment (WEEE) directive and Data Protection Act (DPA).

Portable & Mobile ICT Equipment

This section covers such items as laptops, mobile devices and removable data storage devices. Please refer to the relevant sections of this document when considering storing or transferring personal or sensitive data.

- All activities carried out on school systems and hardware will be monitored in accordance with the general policy.
- Staff must ensure that all school data is stored on the school network, and not kept solely on the laptop. Any equipment where personal data is likely to be stored must be encrypted.
- Equipment must be kept physically secure in accordance with this policy to be covered for insurance purposes. When travelling by car, best practice is to place the laptop in the boot of your car before starting your journey in line with the School's Data Protection Policy.
- Ensure portable and mobile ICT equipment is made available as necessary for anti-virus updates and software installations, patches or upgrades.
- The installation of any applications or software packages must be authorised by the senior ICT technician, fully licensed and only carried out by the ICT technicians.
- In areas where there are likely to be members of the general public, portable or mobile ICT equipment must not be left unattended and, wherever possible, must be kept out of sight.
- Portable equipment must be transported in its protective case if supplied.

19. Mobile technologies

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Mobile technologies such Smartphones, iPads, games players, are generally very familiar to children outside of school. They often provide a collaborative, well-known device with possible internet access and thus open up risk and misuse associated with communication and internet use. Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed. Our school chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

Personal Mobile Devices (including phones)

- The school allows staff to bring in personal mobile phones and devices for their own use.
- Under no circumstances does the school allow a member of staff to contact a student or parent/ carer using their personal device.
- Students are allowed to bring personal mobile devices/phones to school but must not use them for personal purposes within lesson time, apart from 6th form students who, on signing the Online Safety and ICT Acceptable Use agreement, can bring into school their personal device for educational purposes only. At all times the device must be switched off. Mobile devices/phones must not be seen otherwise they'll be confiscated and a detention issued (reference Behaviour Policy).
- This technology may be used for educational purposes, as mutually agreed with the Headteacher. The device user, in this instance, must always ask the prior permission of the bill payer.
- The school is not responsible for the loss, damage or theft of any personal mobile device
- The sending of inappropriate text messages between any member of the school community is not allowed.
- Permission must be sought before any image or sound recordings are made on these devices of any member of the school community.
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

School Provided Mobile Devices (including phones)

- The sending of inappropriate text messages between any member of the school community is not allowed.
- Permission must be sought before any image or sound recordings are made on the devices of any member of the school community.
- Where the school provides mobile technologies such as phones, laptops and iPads for offsite visits and trips, only these devices should be used.
- Where the school provides a laptop for staff, only this device may be used to conduct school business outside of school.
- Never use a hand-held mobile phone whilst driving a vehicle.

20. Social Media, including Facebook and Twitter

Facebook, Instagram, Twitter and other forms of social media are increasingly becoming an important part of our daily lives.

- Our school uses Twitter and Instagram to communicate with parents and carers. Nominated staff, as directed by Assistant Headteacher responsible for e-learning, who have access to these accounts are responsible for all postings for this technology and monitors responses from others.
- New social media accounts requests must be made via the School's online request form located on SharePoint (staff area). Assistant Headteacher responsible for e-learning will approve or decline requests.
- Staff are permitted to access their personal social media accounts using school equipment only during official break times and within designated areas i.e. staff room.
- Staff are able to setup Social Learning Platform accounts, using their school email address, in order to be able to teach students the safe and responsible use of Social Media.
- Students are not permitted to access their social media accounts whilst at school.
- Students in Years 12 & 13 are permitted to access their personal social media account using their own device (i.e. mobile phone) outside of lessons. This is dependent on permission been granted by the Head of 6th form and Assistant Headteacher responsible for e-learning.
- Staff, governors, students, parents and carers are regularly provided with information on how to use social media responsibly and what to do if they are aware of inappropriate use by others.
- Staff, governors, students, parents and carers are aware that the information, comments, images and video they post online can be viewed by others, copied and stay online forever.
- Staff, governors, students, parents and carers are aware that their online behaviour should at all times be compatible with UK law.

21. Systems and Access

- You are responsible for all activity on school systems carried out under any access/account rights assigned to you, whether accessed via school ICT equipment or your own PC.
- Do not allow any unauthorised person to use school ICT facilities and services that have been provided to you.
- Use only your own personal logons, account IDs and passwords and do not allow them to be used by anyone else.
- Keep your screen display out of direct view of any third parties when you are accessing personal, sensitive, confidential or classified information.

- Ensure you lock your screen before moving away from your computer during your normal working day to protect any personal, sensitive, confidential or otherwise classified data and to prevent unauthorised access.
- Ensure that you logoff from the PC completely when you are going to be away from the computer for a longer period of time.
- Do not introduce or propagate viruses.
- It is imperative that you do not access, load, store, post or send from school ICT any material that is, or may be considered to be, illegal, offensive, libellous, pornographic, obscene, defamatory, intimidating, misleading or disruptive to the school or may bring the school into disrepute. This includes, but is not limited to, jokes, chain letters, files, emails, clips or images that are not part of the school's business activities; sexual comments or images, nudity, racial slurs, gender specific comments, or anything that would offend someone on the basis of their age, sexual orientation, religious or political beliefs, national origin, or disability (in accordance with the Sex Discrimination Act, the Race Relations Act and the Disability Discrimination Act).
- Any information held on School systems, hardware or used in relation to School business may be subject to The Freedom of Information Act and The Data Protection Act 2018, namely GDPR (General Data Protection Regulations).
- Where necessary, obtain permission from the owner or owning authority and pay any relevant fees before using, copying or distributing any material that is protected under the Copyright, Designs and Patents Act 1998.
- It is essential that any hard drives which may have held personal or confidential data are 'scrubbed' in way that means the data can no longer be read. It is not sufficient to simply delete the files or reformat the hard drive. Whoever you appoint to dispose of the equipment must provide a written guarantee that they will irretrievably destroy the data by multiple over writing the data.

22. Writing and Reviewing this Policy

Governor Involvement in Policy Creation

- Governors have been involved in making/reviewing the Policy for ICT Acceptable Use through governors sub-committees.

Review Procedure

There will be on-going opportunities for staff to discuss with the Online Safety Coordinator any online safety issue that concerns them.

There will be on-going opportunities for staff to discuss with a member of SLT any issue of data security that concerns them.

This policy will be reviewed every (24) months and consideration will be given to the implications for future whole school development planning.

The policy will be amended if new technologies are adopted or Central Government change the orders or guidance in any way.

23. Links to other Higham Lane School policies

- Child protection and safeguarding policy
- Anti-bullying Policy
- Behaviour for learning policy

- Data Protection Policy
- Staff Code of Conduct Policy
- Remote Learning Policy

24. Current Legislation

Acts Relating to Monitoring of Staff email

Data Protection Act 2018
The Act requires anyone who handles personal information to comply with important data protection principles when treating personal data relating to any living individual. The Act grants individuals rights of access to their personal data, compensation and prevention of processing.
http://www.legislation.gov.uk/ukpga/2018/12/enacted

The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
http://www.hmso.gov.uk/si/si2000/20002699.htm

Incoming and outgoing telephone calls will be recorded from all School telephone extensions and stored securely on a secure server. Parents/carers and other are advised to contact the school either in writing or by email if they would rather their call not recorded.

Regulation of Investigatory Powers Act 2000
Regulating the interception of communications and making it an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIP was enacted to comply with the Human Rights Act 1998. The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, however, permit a degree of monitoring and record keeping, for example, to ensure communications are relevant to school activity or to investigate or detect unauthorised use of the network. Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored. Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation.
http://www.legislation.gov.uk/ukpga/2000/23/contents

Human Rights Act 1998
http://www.legislation.gov.uk/ukpga/1998/42/contents

Other Acts Relating to E-Safety

Racial and Religious Hatred Act 2006
It a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.
http://www.legislation.gov.uk/ukpga/2006/1/contents

Sexual Offences Act 2003
The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence.

Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. Schools should already have a copy of "*Children & Families: Safer from Sexual Crime*" document as part of their child protection packs.
http://www.legislation.gov.uk/ukpga/2003/42/contents

Communications Act 2003 (section 127)

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.
http://www.legislation.gov.uk/ukpga/2003/21/section/127

The Computer Misuse Act 1990 (sections 1 – 3)

Regardless of an individual's motivation, the Act makes it a criminal offence to gain:

- Access to computer files or software without permission (for example using another person's password to access files).
- Unauthorised access, as above, in order to commit a further criminal act (such as fraud).
- Impair the operation of a computer or program.

UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences. http://www.legislation.gov.uk/ukpga/1990/18/section/1
http://www.legislation.gov.uk/ukpga/1990/18/section/2
http://www.legislation.gov.uk/ukpga/1990/18/section/3
http://www.legislation.gov.uk/ukpga/1990/18/section/3ZA
http://www.legislation.gov.uk/ukpga/1990/18/section/3A

Malicious Communications Act 1988 (section 1)

This legislation makes it a criminal offence to send an electronic message (email) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety.
http://www.legislation.gov.uk/ukpga/1988/27/section/1

Copyright, Design and Patents Act 1988

Copyright is the right to prevent others from copying or using work without permission. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer. Copyright infringement is to copy all or a substantial part of anyone's work without obtaining them author's permission. Usually a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else's material. It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.
http://www.legislation.gov.uk/ukpga/1988/48/contents

Public Order Act 1986 (sections 17 – 29)

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence. http://www.legislation.gov.uk/ukpga/1986/64/part/III

Protection of Children Act 1978 (Section 1)
It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.
http://www.legislation.gov.uk/ukpga/1978/37/section/1

Obscene Publications Act 1959 and 1964
Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.
http://www.legislation.gov.uk/ukpga/Eliz2/7-8/66/contents
http://www.legislation.gov.uk/ukpga/1964/74/contents

Protection from Harassment Act 1997
A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other.
A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.
http://www.legislation.gov.uk/ukpga/1997/40/contents

Acts Relating to the Protection of Personal Data

Data Protection Act 2018
http://www.legislation.gov.uk/ukpga/2018/12/enacted

The Freedom of Information Act 2000
https://ico.org.uk/for-organisations/guide-to-freedom-of-information/

Counter-Terrorism and Security Act 2015 (Prevent), Anti-Radicalisation & CounterExtremism Guidance
https://www.gov.uk/government/publications/preventing-extremism-in-schools-and-childrensservices

Higham Lane School
Helping Learners Succeed

Appendix A

Higham Lane School: Process for Monitoring Issues – Grade 1-5

- **Monitor activity on the system:** SH (Steve Holley/ JA Julie Ashley – ICT Development Service) – (Aaron Porter (AP) will cover in this order if SH/JA unavailable).
- **Report to:** KN/NK (Katie Tomlinson/Neetan Kalair, Senior IT Technician/ IT Technician) - then AT Tim Anstey (Online Safety Coordinator), NA Ian Naisbitt, (Assistant Headteacher E-learning), Assistant Headteacher - lead on behaviour, DO Vanessa Domigan (Senior DSL), LW Leanne Whitfield (Deputy Senior DSL) if KN/NK unavailable or requires escalation.

Use the following process when an incident is flagged up by PCE (Policy Central)

GRADE	**Grade 1**	**Grade 2**	**Grade 3**	**Grade 4**	**Grade 5**
Category	False Positive	Noted No immediate action	Reportable Incident	Repeat incident	Major Incident
Type of Incident	No action required	This is of interest but does not require a report unless further activity is observed. SH/JA to search for words over last 2 hrs typed or not.	Type of capture: • Bullying • Unsafe use of Internet • Repeated use of bad language • Attempt to access adult sites • Access to pornographic material by an adult	Repeat incidents at Grade 3 SH/JA to check previous incidents of user and include in the report.	Type of capture: • **Illegal Activity** • **Grooming** • **Threat to Life** • **Access to Pornographic material by a child**
Escalate?		Is it a Grade 3 (further activity observed)? Yes ➔ Confirmed as a grade 2 ↓	Is it a Grade 4 (i.e. repeated activity)? Yes ➔ Confirmed as a grade 3 ↓		Activity identified. **Consensus of opinion required** KN, Online Safety Coordinator, SLT – behaviour, SLT – lead for e-learning and senior/deputy senior DSL or any other senior member of staff if others not available). Confirmed as a grade 5 ↓

Action		If not, no further action required	SH/JA send email to KN/NK with “Grade 3” as subject. KN/NK will receive an email with a password protected report word document through email. KN/NK to record incident through CPOMS which notifies relevant staff - Year group Progress Leader (PL), Senior & Deputy Senior DSL, SLT lead for e-learning & online safety coordinator. Progress Leader to complete Online Safety Incident Record Form (blue form), liaising with SLT – e-learning, SLT – behaviour & online safety coordinator. On completion pass form onto Data team for entry & recording of Online Safety incident (via SIMS). Original incident form retained with copies sent to SLT – behaviour and Online safety coordinator. Additionally, data team to notify KN/NK Online Safety incident logged. KN/NK will delete email correspondence with protected report MS Word document/screenshot uploaded into CPOMS No further action required.	SH/JA send email to KN/NK with “Grade 4” as subject. Follow the action for Grade 3 ←	SH/JA ring & send email “Grade 5” to KN/NK. Has enough data been provided to decide? If not SH/JA check other activity for this user? Once enough data provided then: If still considered a Grade 5 ↓ Contact in person, phone and via email any available nominated staff i.e. , Online Safety Coordinator, SLT – behaviour, SLT – lead for e-learning and senior/deputy senior DSL & relevant Progress Leader immediately. If any of the above are unavailable contact any member of SLT. **Do not email any sexual explicit images (particularly – minors).** Higham Lane School & Warwickshire ICT Development Service (SH/JA) to review the process for grade 5 and amend if necessary. ← If not a grade 5, follow action for appropriate grade.

This is not an exhaustive list and processes will be updated on a regular basis as the service develops.

Key:

Grooming – where it is blatantly not a child talking to the child in school. Obvious exchange of information which they should not be sharing.

Threat to Life – Suggesting self-harm, ending one’s life, threat to another.

Illegal Activity – all activities which break the law including accessing pornographic material including images of children.

Pornographic material – viewing, storing or producing. It is illegal for a child to view pornographic material. It is illegal to access pornographic images of children. Do not email extreme pornographic images to anyone as evidence. This incident indicates that pornographic material is not being filtered out by our system.

Action following a severe incident

Following any Grade 3-5, SH to check any amendments required to PCE (Policy Central) and contact if necessary. Share with Higham Lane School and offer support to the school, as appropriate/requested.

Warwickshire ICT Development Service Contact details:

Steve Holley	(SH)	07957 363458	01926 738349
Julie Ashley	(JA)		01926 738336
Aaron Porter	(AP)		

Appendix B

Dear Parent/Carer

ICT including the internet, email, mobile technologies and online resources have become an important part of learning in our school. We expect all students to be safe and responsible when using any ICT. It is essential that students are aware of Online Safety and know how to stay safe when using any ICT.

Students are expected to read and discuss the agreement overleaf with their parent/carer and then to sign and follow the terms of the agreement. Any concerns or explanation can be discussed with ***Mr. I Naisbitt, Assistant Headteacher.***

Parent/carer signature

We have discussed this document with…………………………………………….. (child's name) and we agree to follow the online safety rules and to support the safe use of ICT at Higham Lane School.

Parent/carer signature ____

Student signature ____

Date ______________________

Acceptable Use Agreement: Students

- I will only use ICT systems in school, including the internet, email, digital video, and mobile technologies for school purposes.
- I shall not disable or cause any damage to the School's equipment, or equipment belonging to others.
- I shall immediately report any damage or faults involving equipment or software, however this may have happened.
- Any damage which is caused by myself, would mean I may be liable for the cost of repair of the equipment
- I will not download or install software on school systems.
- I will only log on to the school network, other systems and resources with my own username and password.
- I will follow the school's ICT security system and not reveal my passwords to anyone and change them regularly.
- Only where applicable I will only use my school email address.
- I will make sure that all ICT communications with students, teachers or others is responsible and sensible.
- I will be responsible for my behaviour when using the Internet. This includes resources I access and the language I use.
- I will not browse, download, upload or forward material that could be considered offensive or illegal, for example material of an inappropriate matter relating to websites concerning safeguarding, radicalisation and extremism. If I accidentally come across any such material I will report it immediately to my teacher.
- I will not give out any personal information such as name, phone number or address. I will not arrange to meet someone unless this is part of a school project approved by my teacher.
- I am only permitted to take images of students and or staff for educational purposes and with the express permission of the relevant member of staff and in the knowledge of the senior ICT technician and Assistant Headteacher responsible for e-learning. This includes school breaks and all occasions when I am in school uniform or when otherwise representing the school
- I will ensure that my online activity, both in school and outside school, will not cause my school, the staff, students or others distress or bring the school community into disrepute, including through uploads of images, video, sounds or texts.
- I will support the school approach to online safety and not upload or add any images, video, sounds or text that could upset any member of the school community.
- I will respect the privacy and ownership of others' work on-line at all times.
- I will not attempt to bypass the internet filtering system.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available to my teachers.
- I will follow the school's policy on mobile phones. I will not use my mobile phone at any point during the school day unless I have had clear authorisation to do by a member of staff.
- I understand that these rules are designed to keep me safe and that if they are not followed, school sanctions will be applied and my parent/carer may be contacted.
- I understand that the wearing of a Smart Watch is prohibited within school at all times.
- I will not sign up to online services until I am old enough to do so.

Social Media Expectations Agreement

- Social media video posts - students are not permitted to record staff / students / school life on their phones and post this on any form of social media whether public or private. Students will risk their place in the sixth form should they do so.
- Abusive social media texts and images - any abusive or discriminatory content in any form of social media risks students losing their place in the sixth form. This includes private social media posts which then become public.

- Bringing the School into disrepute - behaviour outside school that potentially damages the reputation of the School may result in a student losing their place in the Sixth Form. This includes private social media posts which subsequently become public.
- We respect people's identity and do not tolerate discriminatory behaviour and derogatory language whether in public spheres or seemingly private spheres including the following types of discriminatory behaviour: Sexual orientation, Religious Discrimination, National Origin, Sexual Harassment. Students who engage in such behaviour risk their place in the sixth form.

Signed………………………………………….. Parent/ Carer

Pupils are expected to read and discuss this agreement with their parent/ carer and then to sign and follow the terms of the agreement. Any concerns or explanation can be discussed with ***Mr. I Naisbitt, Assistant Headteacher.***

I have read and understand the Online Safety and ICT Acceptable Use Agreement and agree to follow Online Safety rules and to support the safe use of ICT at Higham Lane School.

Name of student ……………………………………………

Signed…………………………………………..

Tutor group …………………………………. Date ………………………………

Appendix C

Staff, Governor and Visitor Acceptable Use Agreement / Code of Conduct

ICT (including data) and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with Mr. I Naisbitt.

- I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed acceptable by the Head or Governing Body.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that all electronic communications with students and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number, personal email address, personal Twitter account, or any other social media link, to students.
- I will only use the approved, secure email system(s) for any school business.
- I will ensure that personal data (such as data held on MIS software) is kept secure and is used appropriately, whether in school or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body. Personal or sensitive data taken off site must be encrypted.
- I will not install any hardware or software without permission of the senior ICT technician.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of students and/ or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member.
- Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Headteacher.
- I will support the school approach to online safety and not upload or add any images, video, sounds or text linked to or associated with the school or its community'.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Headteacher.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring the school, my professional reputation, or that of others, into disrepute.
- I will support and promote the school's Online Safety and Data Security policies and help students to be safe and responsible in their use of ICT and related technologies.
- I will only use my mobile/smart phone in a professional capacity while on school trips including taking images of students and/or staff.
- I will check the School's MIS to verify parents/carers have given consent to their child's image being captured, reproduced and published in accordance to the Data Protection Policy.
- I will not use personal electronic devices (including smart watches) in public areas of the school during the school day.
- I understand authorised ICT staff may inspect any ICT equipment owned or leased by the school at any time without prior notice as set out in the Online Safety and ICT Acceptable Use Policy.
- I understand this forms part of the terms and conditions set out in my contract of employment.

User Signature
I agree to follow this code of conduct and to support the safe and secure use of ICT throughout the school

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

Full Name ……………………………….. (printed)

Job title ……………………………………………………………………

Appendix D

Online Safety and ICT Acceptable Use Agreement: Sixth Form Students

These rules help to protect students and the School Sixth Form by describing acceptable and unacceptable computer use. Further information is contained in the School's Online Safety and ICT Acceptable Use Policy, located on the school's website.

General Use Agreement

- I will only use ICT systems in the Sixth Form, including the internet, email, digital video, and mobile technologies for educational purposes
- I will not download or install software on Sixth Form technologies
- I will only log on to the Sixth Form network, other systems and resources with my own username and password
- I will follow the Sixth Form's ICT security system and not reveal my passwords to anyone and change them regularly.
- I will make sure that all ICT communications with students, teachers or others is responsible and sensible
- I will be responsible for my behaviour when using the internet. This includes resources I access and the language I use
- I will not browse, download, upload or forward material that could be considered offensive or illegal, for example material of an inappropriate matter relating to websites concerning safeguarding, radicalisation and extremism. If I accidentally come across any such material I will report it immediately to my teacher
- I will not give out any personal information such as name, phone number or address. I will not arrange to meet someone unless this is part of a school project approved by my teacher
- I am aware that when I take images of students and/or staff that I must only store and use these for Sixth Form purposes in line with Sixth Form policy and must never distribute these outside the Sixth Form network without the permission of all parties involved. This includes Sixth Form breaks and all occasions when I am representing the Sixth Form
- I will ensure that my online activity, both in Sixth Form and outside the Sixth Form, will not cause the Sixth Form, the staff, students or others distress or bring the Sixth Form community into disrepute, including through uploads of images, video, sounds or texts
- I shall not disable or cause any damage to the Sixth Form's equipment, or equipment belonging to others
- I shall immediately report any damage or faults involving equipment or software, however this may have happened
- Any damage which is caused by myself, would mean I may be liable for the cost of repair of the equipment
- I will support the Sixth Form approach to online safety and not upload or add any images, video, sounds or text that could upset any member of the school community
- I will respect the privacy and ownership of others' work on-line at all times
- I will not attempt to bypass the internet filtering system
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available to my teachers
- I understand that these rules are designed to keep me safe and that if they are not followed, Sixth Form sanctions will be applied and my parent/ carer may be contacted
- I understand that I cannot wear my Smart Watch in an exam or assessment.
- I will not sign up to online services until I am old enough to do so

Bring Your Own Device (BYOD) Agreement

Students wishing to use their personal devices on Higham Lane Sixth Form site must also adhere to the Online Safety and ICT Acceptable Use Policy, Behaviour for Learning Policy and AntiBullying Policy. Please note that students are only allowed one device connected to the school network. If more devices are required, then special permission will need to be gained to allow this.

- I am fully responsible for my device(s). I understand that Higham Lane Sixth Form is not responsible for the device(s) in any way.
- I am not permitted to leave my device(s) on Sixth Form premises outside of Sixth Form hours.
- When not in use for educational purposes my device(s) must be left 'on silent' to prevent any disruption.
- I must immediately comply with any teacher's requests to put away, shut down or close the screen on my device(s).
- I understand that I am not permitted to either transmit or upload photographic images/videos of any person on the Higham Lane Sixth Form site to the internet other than Sixth Form approved sites.
- I am responsible for charging my personal device(s) before bringing it/them to Sixth Form so it/they can run on their batteries whilst at Sixth Form. Charging may not always be available and it will always be at the discretion of teachers.
- I understand that the Higham Lane Sixth Form will not accept any responsibility for damage to my device under any circumstances, including damage caused by connecting to the Sixth Form network and any infection by malware (i.e. viruses, worms, ransomware, spyware, adware, scareware and other malicious programs).
- To ensure appropriate internet filters are in place, I understand that I can only use the Higham Lane Sixth Form Wi-Fi connection in the school network and will not attempt to bypass the network restrictions by using a 3G or 4G network.
- I understand that I must take all reasonable steps to avoid bringing devices onto the Higham Lane Sixth Form site that might infect the network with a virus, worm or any program designed to damage, alter, destroy, or provide access to unauthorized data or information. Failure to do so is in violation of the Online Safety and ICT Acceptable Use Policy and will result in disciplinary action in accordance with the Sixth Form's Behaviour for Learning Policy.
- I accept that the Higham Lane Sixth Form has the right to examine any device that is suspected of causing problems or is the source of an attack or virus infection.
- I understand that if I choose to share the use of my personal device(s) with other students, the device remains my responsibility. I can choose not to share my device.
- I agree that my device(s) cannot be used during tests or assessments of any kind unless otherwise specifically directed by a teacher.

I understand that the use of personal device(s) on the Higham Lane Sixth Form's site is only permitted in so far as it supports my learning and educational experience. It is not a right but a privilege, and I understand that any breach of these rules may lead to the removal of this right at any time and without notice.

I also understand that any breach of these rules may result in other appropriate sanctions. I confirm that I understand and agree to follow the above rules and guidelines.

Wi-Fi Use Agreement

- Only one device is allowed to be connected to the Sixth Form Wi-Fi (unless there are exceptional reasons).
- When your personal device is connected to the Sixth Form network the data transmitted by your device is subject to the same monitoring and filtering as any other Sixth Form device.

- The Sixth Form technical staff cannot offer you support with your personal device beyond helping you connect your device to the Sixth Form network.
- The Sixth Form accepts no liability for any damage to your device or its data that may occur when your device is connected to the Sixth Form network.

Email Use Agreement

- An email account will be provided for you by the Sixth Form.
- I will only use my Sixth Form email address for educational purposes.
- This email account is monitored. You should have no expectation of privacy in any email communication.
- You understand that email is primarily intended for educational use and that you will not use it for personal or recreational use unless you have permission.
- You will not display, transmit, send or print any message, data or image that is likely to cause inconvenience, harassment, alarm or distress to any other person. This is bullying and will not be tolerated (this applies to non-email services as well).
- If you are the recipient of any unwanted message, data or image you must report it to a member of staff (this applies to non-email services as well).
- E-mail filters have been implemented to safeguard the interests of all users of computers and the Internet in the Sixth Form. You will not try to by-pass these filters.
- Misuse of email facilities will not be tolerated. Misuse will likely result in a ban of email and/or internet services. More serious misuse (i.e. bullying) will have more serious consequences
- You will not open any attachments to emails, unless you know and trust the person/organisation who sent the email, due to the risk of the attachment containing viruses or other harmful programmes.
- Automatic scanning of emails and attachments is set to check for viruses, rogue files obscene items, executables, etc.
- Examples of unacceptable use:
  - Producing or relaying SPAM mail
  - Transmission or receipt of large files that may prove detrimental to Sixth Form systems and other users of those systems
- Electronic contact with staff should only take place via Sixth Form sanctioned channels.
- Students may only use Sixth Form approved accounts on the Sixth Form system and only for educational purposes

Remote Desktop Access Agreement

This agreement is to define standards, procedures, and restrictions for connecting to Higham Lane Sixth Form’s internal network(s) from external a host i.e. your home computer. Remote Desktops (access) will be provided for you by the Sixth Form.

- I will only log on to the Sixth Form network, other systems and resources with my own username and password
- You understand that Remote Desktops is primarily intended for educational use and that you will not use it for personal or recreational use unless you have permission.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- Misuse of Remote Desktops facilities will not be tolerated. Misuse will likely result in a ban or complete removal of the facilities.
- I will not install, attempt to install or store programmes of any type on any Sixth Form device, nor will I try to alter computer settings.
- I will not attempt to bypass the internet filtering system
- The Remote Desktops are Sixth Form property and should be treated like a physical computer within the Sixth Form.
- The Remote Desktops are monitored. You should have no expectation of privacy when using them.

- I understand that any breach of these rules may result in other appropriate sanctions. I confirm that I understand and agree to follow the above rules and guidelines.
- It is not a right but a privilege, and I understand that any breach of these rules may lead to the removal of this right at any time and without notice.
- I am responsible for the support, configuration and operation of my own personal computers.
- All expenses related to the use of this service, such as costs for public Internet services, are the responsibility of each individual.
- Approved users of this service are responsible for maintaining the security of their own personal computer systems, for example keeping your account information private and never leaving your personal computer unattended while logged in.
- Due to licencing restrictions not all software will be available on the Remote Desktops.

Every attempt will be made to ensure that Higham Lane Sixth Form's Remote Desktop Access Service remains stable and operational. However, there will be times when the service is unavailable due to system maintenance, or when the number of users logging in exceeds the number of available user licenses, or when there are other unforeseen events or circumstances.

Additional Internet Access Agreement

- The internet access provided by the Sixth Form must only be used for educational purposes.
- You will only use social media sites with permission and at the times that are allowed.
- The Sixth Form has the right to monitor and intercept and/or record any communications made by you using the Sixth Form's internet access. You should have no expectation of privacy in any communication.
- Students accessing inappropriate sites will not be tolerated.
- Web filters are in place for the safety of staff and students. You will not attempt to by-pass these web filters.
- If you become aware that another student has by-passed a filter or that a student is viewing inappropriate web-material you must report it to a member of staff immediately.
- As a Sixth Form student you have access to resources that other students do not (i.e. YouTube). Misuse of these resources will result in a loss of access to these resources.

Students are expected to read and discuss this agreement with their parent/carer and then to sign and follow the terms of the agreement. Any concerns or explanation can be discussed with ***Mr I Naisbitt, Assistant Headteacher.*** Please bring the signed reply slip below and hand it to Sixth Form Reception on <Date>.

This agreement reflects the Sixth Form's Online Safety & ICT Acceptable Use Policy. Please refer to this policy. A copy can be found on the Sixth Form's website under School Policies within School Information.

Appendix E

Higham Lane School Email Protocol (6) – Amended from 14/01/19 following consultation

At Higham Lane School, we seek to ensure staff experience the most effective working experience that is possible and achieve a reasonable work-life balance. Our approach to emails is part of this commitment.

Guideline	Additional notes and Exceptions
Work emails will be sent between 7am and 7pm only. **Work emails will be sent Monday to Friday only**. Staff who wish to write emails at other times can still compose them and save them, then send them at the agreed times. There is a feature on Outlook that offers delayed delivery.	**Exceptions** include a serious safeguarding issue which will be addressed immediately, school closures, staff absence, cover, an OFSTED inspection, urgent information requests on behalf of external agencies (e.g. about Children Looked After). We will also communicate information about school closures and OFSTED via text message. Hopefully, fewer emails will be sent and there will be more face-to-face communication. Care should also be taken with the tone of emails.
Emails should be addressed to the relevant people only. Whole staff emails will be reserved for whole staff issues only. Blanket emails should be avoided unless absolutely necessary.	Staff will be reminded of how to select only staff relevant to a particular student. Admin staff will still need to email all staff if a parent/carer has been phoned by the School and it is not clear which member of staff contacted the parent/carer.
Emails should be as concise as possible. As a guideline, ideally no more than 10 lines in length. It is accepted that some emails will need to be longer than this however. Attachments should also be as concise as possible. Staff will continue to use the subject heading and EOM (End of Message) for correspondence that is short and requires no reply.	
The expectation is that **staff will have a minimum of** 2 working days **to respond to an email** if it is a request for the member of staff to do something. E.g. An email sent at 2pm on Friday would require a reply by 2pm the following Tuesday for staff working on the Monday and Tuesday. Emails requiring a response will be marked: 'Response required'. Where the 2 working days deadline is a concern to the recipient, this should be raised by the recipient with the sender of the email within the 2 working days.	**Where there is a message to phone a parent/carer**, this should be done as soon as possible please and no later than 24 hours after the original phone call from the parent/carer. **Where the Headteacher's PA, Lisa Luke, has contacted a member of staff** regarding their availability for a meeting, the reply should be done as soon as possible, please and not left for 2 working days. Urgent information requests on behalf of external agencies (e.g. about Children Looked After) should be done as soon as possible, please and not left for 2 working days.
Part-time staff are only expected to read and respond to emails on their working days.	

Appendix F – Online Safety Incident Reporting Form

Section 1 (*Staff member to complete. On completion pass onto the Data Team for SIMS entry*)

Staff code:		**Date:**	
Student name:		**Tutor Group:**	

Date of incident:		**Time of incident:**	

Details of incident (for student file): PLEASE CIRCLE THE TYPE(S) OF INCIDENT IF POSSIBLE (see overleaf for descriptions of incidents)										
A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K*(give details below)**
Details:										

Section 2 (*to be entered on SIMS*) Authorised by: (member of SLT)

Incident type:	**(use description from list overleaf only)**		
Time of incident:		**Activity:**	
Date(s) for sanction: (if applicable)		**Staff code of person entering on SIMS:**	

Action taken: (circle and add no. of hours/days where appropriate)	Verbal reprimand	Lunch DT	Break DT
	School DT	Pastoral DT	Other DT (no. of hours):
	Isolation (no. of days):	Internal exclusion (no. of days)	External exclusion (no. of days):
	Access to internet in school denied	Parent taking action	Other

Comments:	

Parents informed? (circle)	**Yes / No**	**Phone call / Letter home?**	

Additional action:	

Please pass a copy to the Online Safety Coordinator, to the Designated Safeguarding Lead (DSL) and the Data team (who will enter this onto SIMS).

A. Sharing own/using another person’s name/password
B. Disclosing personal information (own or other’s)
C. Using a mobile phone or other device to take a video/ photos/ screenshots etc. without permission
D. Distributing/editing images (self or others) without permission
E. Accessing websites which are against school policy e.g. games
F. Compromising the School ICT network e.g. downloading/uploading/installing anything without permission
G. Copying, removing or editing another user’s file
H. Inappropriate online/other electronic communication
I. Using technology to bully someone
J. Infringement of copyright e.g. music/video downloads, passing off work as your own
K. Other (give details)

Appendix G LAPTOP AGREEMENT FOR STUDENTS

Student **MUST** sign a copy of this Laptop Agreement in order for the Laptop to be issued by the **S4L Department**

This agreement is designed to act as a guide and framework upon which the use of laptops by Students should be based. This loan is subject to review on a regular basis, and can be withdrawn at any time.

The intended spirit of the list is to act as a reminder on use and security.

1. The Laptop and any accessories provided with it remain the property of Higham Lane School and is strictly for use in the assistance of learning. It is an educational resource only. The equipment is to be used in accordance with the terms of the Laptop Agreement.

2. I agree to only use software licensed by the School. Software should only be installed by the ICT Technical Staff. Do not load games or other inappropriate material onto the Laptop. Do not delete any existing software.

3. I agree to treat the Laptop with due care and keep the laptop in good condition, ensure that it is strapped in to the carry case when transported and/or not in use. I am expected to take additional sensible precautions to ensure the safety of the equipment i.e. never leave it unattended. Further to this, that I should take the additional precaution of locking it away in a secure location at the end of the school day – returning it to the Support for Learning department. If S4L department is unavailable please return the laptop to Students Services or the IT Technician office. Equipment must be returned in the same state as when loaned out.

4. The user is responsible for the care of the Laptop for the duration of the loan; consequently you will be held responsible for any damage and may be charged the full cost of repair or replacement or be asked to contribute to such costs. Should any faults occur, I agree to notify the School's ICT Technical Staff/S4L DEPT as soon as possible so that they may undertake any necessary repairs. Under no circumstances should I, or any other person other than the School's ICT Technical Staff, attempt to fix suspected hardware, or any other faults.

5. Anti-virus software is provided with each laptop. If the software is not updating, I am responsible for informing the ICT Technical Staff about the issue.

6. I understand the School will not accept responsibility for the loss of work in the event of the laptop malfunctioning.

7. I will avoid food and drink near the keyboard/touchpad.

8. There are a number of legal requirements relating to the use of information and software (e.g. Data Protection Act (2018), Computer Misuse Act (1990), Copyright, Designs and Patents Act (1988)). I am responsible for understanding and complying with their legal requirements. These laws can be accessed through the government's legislative website - http://www.legislation.gov.uk.

9. I agree I am still fully responsible for the Laptop loaned to myself.

10. Anything saved onto the hard disc will be wiped when the Laptop is returned.

11. As is professional practice, please check all equipment upon issue and report any problems immediately to the ICT Technical Staff/ S4L DEPT. Failure to do so may result in you being held responsible for any damage noted on return of your loan period.

Loan Start Date: ______________________ Loan Length: ________________

I acknowledge receipt of the following equipment:-

Make/Model ______________________ Laptop Name ________________

Charger/Power Adapter Yes ☐ / No ☐ Laptop Bag/Carry Case Yes ☐ / No ☐

Laptop Serial Number ______________________________

Student **AND** Parent or Carer **MUST** sign a copy of this Laptop Agreement in order for the Laptop to be issued by the S4L Department.

Student Name ______________________________

Student Signature ____ Date _____________

Parent/Carer Name ______________________________________

Parent/Carer Signature ____________________________________ Date _____________

Staff/Department Issuing Laptop ____

Reason for issue ____

Staff Signature ____ Date _____________

School Use

Laptop Condition on Issue	Laptop Condition on Return

Appendix H LAPTOP AGREEMENT FOR STUDENTS – LOAN OF LAPTOPS FROM THE LIBRARY

Student **MUST** sign a copy of this Laptop Agreement in order for the Laptop to be issued by the **Health & Safety Officer**

This agreement is designed to act as a guide and framework upon which the use of laptops by Students should be based. This loan is subject to review on a regular basis, and can be withdrawn at any time.

The intended spirit of the list is to act as a reminder on use and security.

1. The Laptop and any accessories provided with it remain the property of Higham Lane School and is strictly for use in the assistance of learning. It is an educational resource only. The equipment is to be used in accordance with the terms of the Laptop Agreement.

2. I agree to only use software licensed by the School. Software should only be installed by the ICT Technical Staff. Do not load games or other inappropriate material onto the Laptop. Do not delete any existing software.

3. I agree to treat the Laptop with due care and keep the laptop in good condition, ensure that it is strapped in to the carry case when transported and/or not in use. I am expected to take additional sensible precautions to ensure the safety of the equipment i.e. never leave it unattended. Further to this, that I should take the additional precaution of locking it away in a secure location at the end of the school day – returning it to the Library. If Library is unavailable please return the laptop to Students Services or the IT Technician office. Equipment must be returned in the same state as when loaned out.

4. The user is responsible for the care of the Laptop for the duration of the loan; consequently you will be held responsible for any damage and may be charged the full cost of repair or replacement or be asked to contribute to such costs. Should any faults occur, I agree to notify the School's ICT Technical Staff/Library as soon as possible so that they may undertake any necessary repairs. Under no circumstances should I, or any other person other than the School's ICT Technical Staff, attempt to fix suspected hardware, or any other faults.

5. Anti-virus software is provided with each laptop. If the software is not updating, I am responsible for informing the ICT Technical Staff about the issue.

6. I understand the School will not accept responsibility for the loss of work in the event of the laptop malfunctioning.

7. I will avoid food and drink near the keyboard/touchpad.

8. There are a number of legal requirements relating to the use of information and software (e.g. Data Protection Act (2018), Computer Misuse Act (1990), Copyright, Designs and Patents Act (1988)). I am responsible for understanding and complying with their legal requirements. These laws can be accessed through the government's legislative website - http://www.legislation.gov.uk.

9. I agree I am still fully responsible for the Laptop loaned to myself.

10. Anything saved onto the hard disc will be wiped when the Laptop is returned.

11. As is professional practice, please check all equipment upon issue and report any problems immediately to the ICT Technical Staff/Library. Failure to do so may result in you being held responsible for any damage noted on return of your loan period.

Loan Start Date: ______________________________ Loan Length: ______________________

I acknowledge receipt of the following equipment:-

Make/Model ________________________________ Laptop Name _________________________

Charger/Power Adapter Yes □ / No □ Laptop Bag/Carry Case Yes □ / No □

Laptop Serial Number ______________________________________

Student **AND** Parent or Carer **MUST** sign a copy of this Laptop Agreement in order for the Laptop to be issued by the Health & Safety Officer or Library Staff.

Student Name ____

Student Signature ____ Date _______________

Parent/Carer Name ____

Parent/Carer Signature ____________________________________ Date_______________

Staff/Department Issuing Laptop ____

Reason for issue____

Staff Signature ____ Date_______________

Date of Issue ______________________________________

School Use

Laptop Condition on Issue	Laptop Condition on Return

Appendix I LAPTOP AGREEMENT - FOR STUDENTS/PARENTS/CARERS

Student **AND** Parent or Carer **MUST** sign a copy of this Laptop Agreement in order for the Laptop to be issued by the School ICT Technicians.

This agreement is designed to act as a guide and framework upon which the use of laptops by Students/Parents/Carers should be based. This loan is subject to review on a regular basis, and can be withdrawn at any time.

The intended spirit of the list is to act as a reminder on use and security.

1. The Laptop and any accessories provided with it remain the property of Higham Lane School and is strictly for use in the assistance of learning. It is an educational resource only. The equipment is to be used in accordance with the terms of the Laptop Agreement.

2. I agree to treat the Laptop with due care and keep the laptop in good condition, ensure that it is strapped in to the carry case (if provided) when transported and/or not in use. I am expected to take additional sensible precautions to ensure the safety of the equipment when left unattended. I should not leave the Laptop on display in any classroom overnight or during the school holidays. Further to this, that I should take the additional precaution of locking it away whether at home or at school. I will avoid food and drink near the keyboard/touchpad. Equipment must be returned in the same state as when loaned out.

3. The user is responsible for the care of the Laptop for the duration of the loan; consequently you will be held responsible for any damage and may be charged the full cost of repair or replacement or be asked to contribute to such costs. Should any faults occur, I agree to notify the School ICT Technical Staff as soon as possible so that they may undertake any necessary repairs. Under no circumstances should I, or any other person other than the School ICT Technical Staff, attempt to fix suspected hardware, or any other faults. **Please Note: The School will undertake regular maintenance checks to ensure the laptop is in a good working condition. Prior notice will be given of when the laptop will be called in. It is the School's intention to inspect the laptop on a termly basis.**

4. Students/Parents/Carers should make sure that they are aware of the arrangements that have been made by the school for insurance cover on Laptops and follow any guidelines/procedures established by the school to safeguard this cover. Where such guidelines/procedures are not followed and the laptop is 'lost', the individual is responsible for the cost of replacing the laptop. This includes, for example, if the laptop is lost at school, lost or stolen from home or if the laptop is stolen from other venues away from school. Any theft should be immediately reported to the police and a crime reference number should be obtained and provided to the Senior ICT Technician and to the Director of Corporate Services.

5. Students/Parents/Carers are free to choose their own ISP and are responsible for any charges incurred. Internet access and use is the responsibility of parents/carers and as such Higham Lane School is not responsible of the conduct of those that loan the laptop. I understand the school will not accept responsibility for offering technical support relating to home Internet connectivity.

6. Anti-virus software is provided with each laptop. If the software is not updating, I am responsible for informing the ICT Technical Staff about the issue.

7. Students should always password protect important or sensitive information, and ensure that back-up copies of such information are taken and held securely. I understand the School will not accept responsibility for the loss of work in the event of the laptop malfunctioning.

8. There are a number of legal requirements relating to the use of information and software (e.g. Data Protection Act (2018), Computer Misuse Act (1990), Copyright, Designs and Patents Act (1988)). I am responsible for understanding and complying with their legal requirements. These laws can be accessed through the government's legislative website - www.legislation.gov.uk

9. I agree to only use software licensed by the School. Software should only be installed by the ICT Technical

Staff. In the event that you wish to load a software package for educational use please seek permission from the School. Do not load games or other inappropriate material onto the Laptop. Do not delete any existing software.

10. I agree I am still fully responsible for the Laptop loaned to myself. I understand however I am still liable for the Laptop.
11. Anything saved onto the hard disc will be wiped when the Laptop is returned.
12. As is professional practice, please check all equipment upon issue and report any problems immediately to the ICT Technical Staff. Failure to do so may result in you being held responsible for any damage noted on return of your loan period.

I acknowledge receipt of the following equipment: -

Make ________________________ Model _____________________

Laptop Name _____________ Laptop Serial Number ______

Charger/Power Adapter Yes ☑ / No ☐ Laptop Bag/Carry Case Yes ☑ / No ☐

Other Items ____

Student **AND** Parent or Carer **MUST** sign a copy of this Laptop Agreement in order for the Laptop to be issued by the School's Senior ICT Technician.

Please Note: This Laptop must be returned to Higham Lane School no later than the <u>end Year 11 or if they should leave Higham Lane School before this time</u>

Student Name ____

Student Signature ____ Date ____________________

Parent/Carer Name ____

Parent/Carer Signature ______________________________________Date ____________________

Staff/Department Issuing Laptop ____

Staff Signature ____ Date ____________________

Date of Issue ______________________________________

Office Use

Laptop Condition on Issue Good working condition – NK Dec 2021	Laptop Condition on Return