Tannery Drift
First School

Enjoyment — Achievement — Respect

eSafety & Data Security Policy

Last Review Date:
December 2020

Next Review Date:
December 2022

Artsmark Gold Award
Awarded by Arts Council England

www.tannerydrift.herts.sch.uk

eSafety & Data Security Policy

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; web-based 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
- E-mail, Instant Messaging and chat rooms
- Social Media, including Facebook and Twitter
- 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
- 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 Tannery Drift First School, we understand the responsibility to educate our pupils on eSafety Issues; 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 sensitive 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.

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 pupils) 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 pupils 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, e-mails, instant messaging, internet/intranet use and any other electronic communications (data, voice, video or image) involving its pupils, 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, acceptable use agreement, standards and procedures; to ensure the effective operation of school ICT; for quality control or training purposes; to comply with a Subject Access Request under the General Data Protection Regulations (GDPR), or to prevent or detect crime.

ICT authorised staff may, without prior notice, access the e-mail or voice-mail 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 GDPR, 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.

3. Breaches

A breach or suspected breach of policy by a school employee, contractor or pupil may result in the temporary or permanent withdrawal of school ICT hardware, software or services from the offending individual.

- Conduct assessments to check organisations are complying with the Act;
- Serve information notices requiring organisations to provide the Information Commissioner's Office with specified information within a certain time period;
- Serve enforcement notices and 'stop now' orders where there has been a breach of the Act, requiring organisations to take (or refrain from taking) specified steps in order to ensure they comply with the law;

- Prosecute those who commit criminal offences under the Act;
- Conduct audits to assess whether organisations' processing of personal data follows good practice,
- Report to Parliament on data protection issues of concern.

3.1 Incident Reporting

Any safeguarding concerns should be reported to The Designated Senior Person, Anna Greetham, or Deputy Designated Senior Person, Roz Torres, Beth Robins and Beth Kerr.

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, Anna Greetham.

Additionally, all security breaches, lost/stolen equipment or data (including remote access SecureID tokens and PINs), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance that may result in a data breach, must be reported to the Data Protection Officer (DPO), Pip McLachlan.

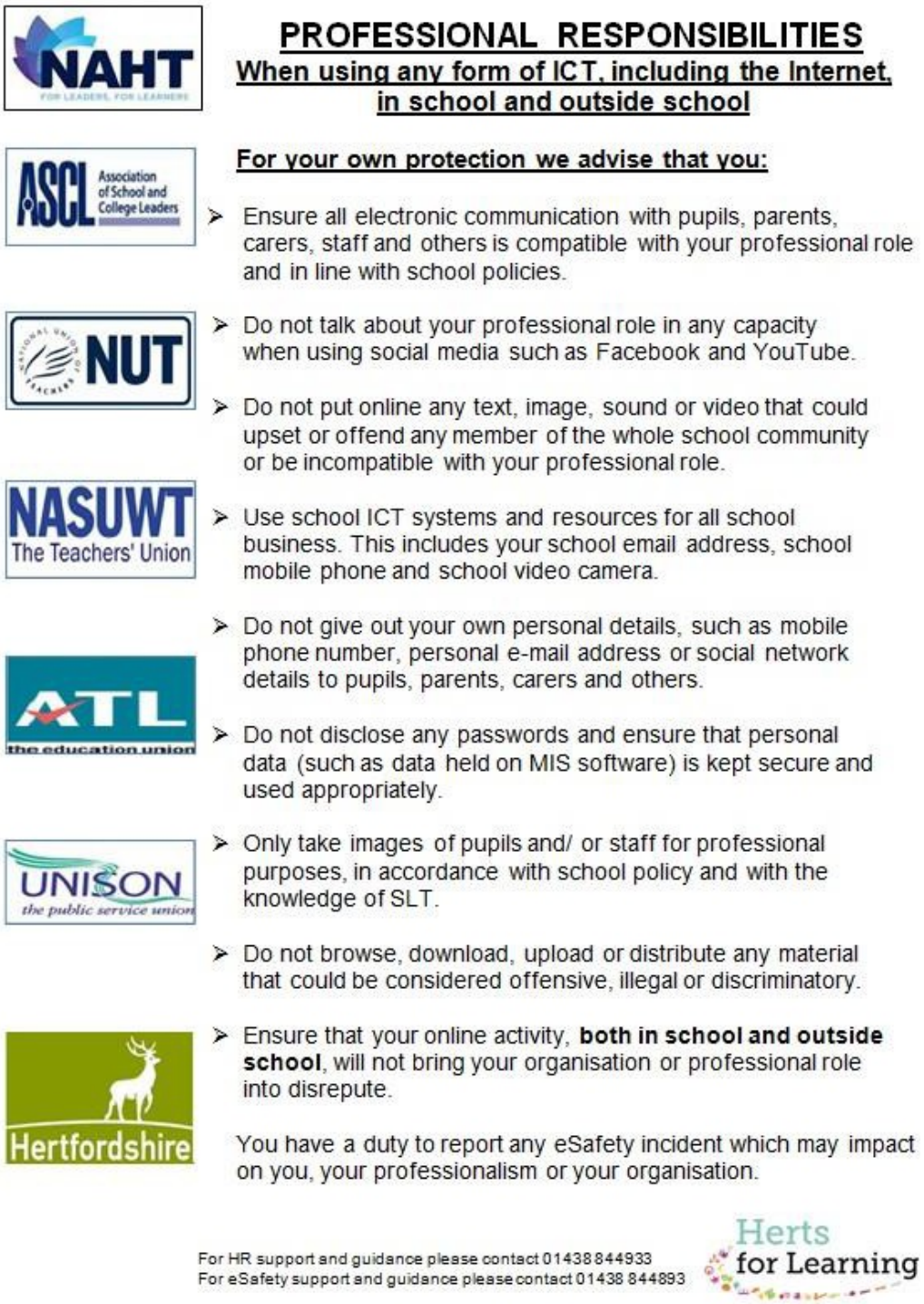
3.2 eSafety Incident Log

An eSafety Incident Log will be kept by the School Business Manager. Any reported events will be recorded in the incident log.

4. Acceptable Use Agreements

Acceptable use agreements are to be signed by all pupils, staff (including governors), and visitors who will have access to ICT resources and equipment.

5. Staff Professional Responsibilities



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 pupils, 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 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 pupils, 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 pupils and/ or staff for professional purposes, in accordance with school 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 your organisation or professional role into disrepute.

You have a duty to report any eSafety incident which may impact on you, your professionalism or your organisation.

For HR support and guidance please contact 01438 844933
For eSafety support and guidance please contact 01438 844893

6. Computer Viruses

- All files downloaded from the Internet, received via e-mail or on removable media such as a memory stick must be checked for any viruses using school provided anti-virus software before being used.
- Never interfere with any anti-virus software installed on school ICT equipment.
- If your machine is not routinely connected to the school network, you must make provision for regular virus updates through your IT team.

- If you suspect there may be a virus on any school ICT equipment, stop using the equipment and contact your ICT support provider immediately. The ICT support provider will advise you what actions to take and be responsible for advising others that need to know.

7. Data Security

The accessing and appropriate use of school data is something that the school takes very seriously.

7.1 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. Where this is not possible, keep it locked out of sight.
- Staff should always keep portable and mobile ICT equipment under your control at all times.
- The usage of removable storage media should be avoided. Where it is essential to use such devices these must be password protected.
- It is the responsibility of individual staff to ensure the security of any personal, sensitive, confidential and classified information contained in documents copied, scanned or printed. This is particularly important when shared printing devices are used.
- Refer to section 10 for email security.

7.2 Handling of Official Information

Official information is handed directly to the relevant staff member at a time when they can deal with it immediately. Staff must be trained to understand that they are personally responsible for securely handling any information that is entrusted to them.

8. Disposal of Redundant ICT Equipment

- Redundant ICT Equipment will all be disposed of in accordance with the WEEE (Waste Electrical and Electronic Equipment) directive (PRM Green Technologies is recommended by Herts for Learning and offers a free service to Hertfordshire schools).
- School will maintain a comprehensive inventory of ICT equipment and records of all disposals.

9. Email

The use of e-mail within most schools is an essential means of communication for both staff and pupils. In the context of school, e-mail should not be considered private. Educationally, e-mail can offer significant benefits including; direct written contact between schools on different projects, be they staff based or pupil based, within school or international. We recognise that pupils need to understand how to style an e-mail in relation to their age and how to behave responsible online.

- The school gives all their staff 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.
- Staff should use their school email for all professional communication.
- Governors should use GovernorHub for all sensitive school related 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 pupils, parents or conduct any school business using personal email addresses.
- The school requires a standard disclaimer to be attached to all email correspondence, stating that, 'the views expressed are not necessarily those of the school or the LA'. The responsibility for adding this disclaimer lies with the account holder.
- 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 to external organisations, parents or pupils are advised to cc. the Headteacher, line manager or designated line manager.
- Pupils 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 the member of staff's school job will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000. Staff must therefore actively manage their email account as follows:
    - Delete all emails of short-term value.
    - Organise email into folders and carry out frequent housekeeping on all folders and archives.
- All pupil email users are expected to adhere to the generally accepted rules of responsible online behaviour particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in e-mail communication, or arrange to meet anyone without specific permission, virus checking attachments.
- Pupils must immediately tell a teacher or trusted adult if they receive an offensive or upsetting email.
- Staff must inform the eSafety co-ordinator or their line manager if they receive an offensive email.

- Pupils are introduced to email as part of the Computing Programme of Study.
- However you access your school e-mail (whether directly, through webmail when away from the office or on non-school hardware) all the school email policies apply.

9.1 Sending Email

- If sending emails containing personal, confidential, classified or financially sensitive data to external third parties or agencies, refer to the Section 'emailing Personal, Sensitive, Confidential or Classified Information'.
- Use your own school email account so that you are clearly identified as the originator of a message.
- 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.

9.2 Receiving Email

- Check your email regularly.
- Activate your 'out-of-office' notification when away for extended periods.
- Never open attachments from an untrusted source; consult your network manager first.
- 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.

10. Emailing Personal, Sensitive, Confidential or Classified Information

Where your conclusion is that e-mail must be used to transmit such data, either:
Obtain express consent from your manager to provide the information by e-mail and exercise caution when sending the e-mail and always follow these checks before releasing the e-mail:

- Encrypt and password protect.
- Verify the details, including accurate email address, of any intended recipient of the information.
- Verify (by phoning) the details of a requestor before responding to email requests for information.
- Do not copy or forward the email to any more recipients than is absolutely necessary.
- Do not send the information to any person whose details you have been unable to separately verify (usually by phone).

- Send the information as an encrypted document **attached** to an email Provide the encryption key or password by a **separate** contact with the recipient(s).
- Do not identify such information in the subject line of any email.
- Request confirmation of safe receipt.

Or:
Use Hertsfx or Schoolsfx, Hertfordshire's web-based Secure File Exchange portal that enables schools to send and receive confidential files securely.
http://www.thegrid.org.uk/eservices/schoolsfx.shtml

11. Equal Opportunities

11.1 Pupils with Additional Needs

The school endeavours to create a consistent message with parents/carers for all pupils and this in turn should aid establishment and future development of the schools' eSafety rules. However, staff are aware that some pupils may require additional support or teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of eSafety issues.

Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of eSafety. Internet activities are planned and well managed for these children and young people.

12. eSafety

12.1 eSafety - Roles and Responsibilities

As eSafety 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 eSafety co-ordinator in this school is the Computing Subject Leader. All members of the school community have been made aware of who holds this post. It is the role of the eSafety co-ordinator to keep abreast of current issues and guidance through organisations such as Herts LA, Herts for Learning Ltd, CEOP (Child Exploitation and Online Protection) and Childnet.

Senior Management and governors are updated by the Headteacher / eSafety co-ordinator and all governors have an understanding of the issues and strategies at our school in relation to local and national guidelines and advice.

12.2 eSafety in the Curriculum

Tannery Drift First School recognises that internet, mobile and digital technologies provide positive opportunities for children and young people to learn, socialise and play but they also need to understand the challenges and risks.

The digital world is an amazing place, but with few rules. It is vast and fast moving and young people's future economic success may be partly dependent on their online skills and reputation. We are, therefore, committed to ensuring that all pupils, staff and governors will be supported to use internet, mobile and digital technologies safely. This is part of our safeguarding responsibility.

- The school has a framework for teaching internet skills in computing lessons, which can be found on the staff server.
- The school provides opportunities within a range of curriculum areas to teach about eSafety.
- Educating pupils about the online risks that they may encounter outside school is done informally when opportunities arise and as part of the eSafety curriculum.
- Pupils are taught about copyright, respecting other people's information, safe use of images and other important areas through discussion, modelling and appropriate activities.
- Pupils are aware of the impact of Cyberbullying and know how to seek help if they are affected by any form of online bullying. Pupils 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 Cybermentors, Childline or CEOP report abuse button.
- Pupils are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the Computing curriculum.

12.3 eSafety Skills Development for Staff

- Our staff receive regular information and training on eSafety and how they can promote the 'Stay Safe' online messages in the form of staff briefings and newsletters.
- Details of the ongoing staff training programme can be found in the Business Manager Training Log.
- New staff sign the school's acceptable use agreement 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 eSafety.
- All staff are encouraged to incorporate eSafety activities and awareness within their curriculum areas and ensure they are adequately informed with up-to-date areas of concern.

12.4 Managing the School eSafety Messages

We endeavour to embed eSafety messages across the curriculum whenever the internet and/or related technologies are used.

- The eSafety policy will be introduced to the pupils at the start of each school year.
- eSafety posters will be prominently displayed.
- The key eSafety advice will be promoted widely through school displays, newsletters, class activities and so on.
- We will participate in Safer Internet Day every February.

13. eSafety Incident Reporting, Incident Log and Infringement

13.1 Incident Reporting

Any safeguarding concerns should be reported to The Designated Senior Person, Anna Greetham, or Deputy Designated Senior Person, Roz Torres, Beth Robins or Beth Kerr.

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, Anna Greetham.

Additionally, all security breaches, lost/stolen equipment or data (including remote access SecureID tokens and PINs), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance that may result in a data breach, must be reported to the Data Protection Officer (DPO), Pip McLachlan.

13.2 eSafety Incident Log

An eSafety Incident Log will be kept by the School Business Manager. An incident log template can be downloaded from: http://www.thegrid.org.uk/eservices/safety/incident.shtml

Any reported events will be recorded in an incident log.

14. Misuse and Infringements

14.1 Complaints

Complaints and/ or issues relating to eSafety should be made to the Headteacher.

14.2 Inappropriate Material

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the eSafety co-ordinator.
- Deliberate access to inappropriate materials by any user will lead to the incident being reported to the 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 in the Staff Handbook.

15. 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 through the HICS network (Hertfordshire Internet Connectivity Service) is logged and the logs are randomly but regularly monitored. Whenever any inappropriate use is detected it will be followed up.

15.1 Managing the Internet

- The school provides pupils with supervised access to internet resources (where reasonable) through the school's fixed and wireless 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 pupils.
- 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.

15.2 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, pupils, 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 pupils and how this is disseminated.

15.3 Infrastructure

- Hertfordshire Local Authority has a monitoring solution via the Hertfordshire Grid for Learning where web-based activity is monitored and recorded.
- School internet access is controlled through the HICS web filtering service.
- Tannery Drift First School is aware of its responsibility when monitoring staff communication under current legislation and takes into account; GDPR, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Regulation of Investigatory Powers Act 2000, Human Rights Act 1998.
- Staff and pupils are aware that school based email and internet activity can be monitored and explored further if required.
- The school does not allow pupils access to internet logs.
- The school uses management control tools for controlling and monitoring workstations.
- If staff or pupils discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to the e- safety coordinator or teacher as appropriate.
- It is the responsibility of the school, by delegation to the network manager, to ensure that anti-virus protection is installed and kept up- to-date on all school machines.

- Pupils and staff are not permitted to download programs or files on school based technologies without seeking prior permission from the Computing Subject Leader.
- If there are any issues related to viruses or anti-virus software, the network manager should be informed via the Computing Subject Leader.

16. 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 pupils to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.

- All pupils are advised to be cautious about the information given by others on such websites, for example users not being who they say they are.
- Pupils 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.
- Pupils are always reminded to avoid giving out personal details on websites which may identify them or where they are (full name, address, mobile/interests.
- Our pupils are advised to set and maintain their online profiles to maximum privacy and deny access to unknown individuals.
- Pupils are encouraged to be wary about publishing specific and detailed private thoughts and information online.
- Our pupils are asked to report any incidents of cyberbullying to the school.
- Staff may only create blogs, wikis or other online areas in order to communicate with pupils using the school learning platform or other systems approved by the Headteacher.
- Services such as Facebook and Instagram have a 13+ age rating which should not be ignored.

17. Working in Partnership with Parents & Carers

The school works closely with families to help ensure that children can use internet, mobile and digital technologies safely and responsibly both at home and school. The support of parents/carers is essential to implement the online safety policy effectively and help keep children safe.

It is important that parents/carers understand the crucial role they play in this process. The school seeks to regularly consult and discuss online safety with parents/carers and seeks to promote a wide understanding of the benefits of new technologies and associated risks. The school provides regular updated online safety information through the school website, newsletters and by other means.

Parents/carers are asked on an annual basis to read, discuss and co-sign with each child the Acceptable Use Agreement. A summary of key parent/carer responsibilities will also be provided and is available in Appendix F. Personalise as required. The Acceptable Use Agreement explains the school's expectations and pupil and parent/carer responsibilities.

- 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).
- Parents/carers are expected to sign a Home School agreement.
- The school disseminates information to parents relating to eSafety where appropriate in the form of:
  - Information evenings.
  - Practical training sessions e.g. current eSafety issues.
  - Posters.
  - School website information.
  - Newsletter items.

18. Passwords and Password Security

18.1 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 Deputy Headteacher or School Business Manager 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.

18.2 Password Security

- Password security is essential for staff, particularly as they are able to access and use pupil data. Staff are expected to have secure passwords which are not shared with anyone. The pupils are expected to keep their passwords private and not to share with others, particularly their friends. Staff and pupils 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 e-Safety Policy and Data Security.

- Users are provided with an individual network and email log-in username. They are also expected to use a personal password and keep it private.

- Pupils are not allowed to deliberately access on-line 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, MIS systems and/or learning platform, 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 log-off time for the school network is 9pm.

19. Zombie Accounts

Zombie accounts refers to accounts belonging to users who have left the school and therefore no longer have authorised access to the school's systems. Such Zombie accounts when left active can cause a security threat by allowing unauthorised access.

- Ensure that all user accounts are disabled once the member of the school has left.

- Prompt action on disabling accounts will prevent unauthorized access.

- Regularly change generic passwords to avoid unauthorised access.

20. Personal or Sensitive Information

20.1 Protecting Personal, Sensitive, Confidential and Classified Information

- Ensure that any school information accessed from your own PC or removable media equipment is kept secure, and remove any portable media from computers when not attended.

- 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, sensitive, confidential and classified information you disclose or share with others.

- Ensure that personal, sensitive, confidential or classified information is not disclosed to any unauthorised person.

- Ensure the security of any personal, sensitive, confidential and classified information contained in documents you copy, scan or print. This is particularly important when shared printing devices are used and when access is from a non-school environment.

- Only download personal data from systems if expressly authorised to do so by your manager.
- You must not post on the internet personal, sensitive, confidential, or classified 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.

20.2 Storing/Transferring Personal, Sensitive, Confidential or Classified Information Using Removable Media

- Ensure removable media is purchased with encryption.
- Store all removable media securely.
- Ensure hard drives from machines no longer in service are removed and stored securely or wiped clean.
- Always consider if an alternative solution already exists.
- Only use recommended removable media.
- Encrypt and password protect.
- Store all removable media securely.
- Removable media must be disposed of securely by your ICT support team.

21. Remote Access

- You are responsible for all activity via LARA (Login Anywhere Remote Access).
- Only use equipment with an appropriate level of security for remote access.
- To prevent unauthorised access to school systems, keep logon IDs and passwords confidential and do not disclose them to anyone.
- Avoid writing down or otherwise recording any network access information.
- Protect school information and data at all times, including any printed material. Take particular care when access is from a non-school environment.

22. Safe Use of Images

22.1 Taking of Images and Film

Photographs and videos provide valuable evidence of pupils' achievement and progress in a variety of contexts and can be used to celebrate the work of the school. In line with GDPR they are used only with the written consent of parents/carers which is secured in the first instance on a child's entry to the school.

Records are kept on file and consent can be changed by parents/carers at any time.

Photographs and images of pupils are only stored on the school's agreed secure networks which include some cloud based services. Rights of access to stored images are restricted to approved staff as determined by the Headteacher. Staff and pupils may have temporary access to photographs taken during a class session, but these will be transferred/deleted promptly.

Parents/carers should note that there may be some children who are at risk and must not have their image put online and others who do not want their image online. For these reasons parents/carers must follow the school's Acceptable Use Agreement and refrain from taking or posting online photographs of any member of the school community, other than their own child/ren.

Staff and other professionals working with pupils, must only use school equipment to record images of pupils whether on or off site. Permission to use images of all staff who work at the school is sought on induction and a written record is located in the personnel file.

22.2 Consent of Adults Who Work at the School

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

22.3 Publishing Pupil's Images and Work

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

- on the school website.
- in the school prospectus and other printed publications that the school may produce for promotional purposes.
- on the school's private Twitter account.
- recorded/ transmitted on a video or webcam.
- shared via the school's locked YouTube account.
- on the school's learning platform or Virtual Learning Environment.
- 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 or a change in how images may be used.

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.

Pupils' names will not be published alongside their image and vice versa. Email and postal addresses of pupils will not be published. Pupils' full names will not be published.

Before posting named student work on the Internet, a check needs to be made to ensure that permission has been given for work to be displayed.

For further information relating to issues associated with school websites and the safe use of images in Hertfordshire schools, see:

22.4 Storage of Images

- Images/ films of children are stored on the school's network.
- Pupils and staff are not permitted to use personal portable media for storage of images (e.g. USB sticks) without the express permission of the Headteacher.
- Rights of access to this material are restricted to the teaching staff within the confines of the school network or other online school resource.
- Teaching Staff, including the Computing Subject Leader have the responsibility of deleting the images when they are no longer required, or when the pupil has left the school.

22.5 Other Methods for Transfer and Storage of Images

In order to facilitate photography of school activities and events by designated volunteers who are not members of school staff, the Headteacher may agree, in writing, working methods and practices for the production, storage, transfer of images outside of the normal policy. The methods and practices agreed will ensure:

- Images must be securely stored (password protected and/or encrypted).
- Images must not be uploaded to the internet.
- Images must not be shared with a third party without the Headteacher's consent.
- Images must be transferred in a secure way.

Such agreements will be detailed in the Annual Safeguarding Checklist.

22.6 Webcams

- 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).
- Consent is sought from parents/carers and staff on joining the school, in the same way as for all images.
- 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.

22.7 Video Conferencing

- Permission is sought from parents and carers if their children are involved in video conferences with end-points outside of the school.
- All pupils 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.
- The school conferencing equipment is not set to auto-answer and is only switched on for scheduled and approved conferences.
- 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 (previously CRB) 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.

23. School ICT Equipment including Portable & Mobile ICT Equipment & Removable Media

23.1 School ICT Equipment

- It is recommended that schools log 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.
- All staff are responsible for ensuring that all ICT equipment used is kept physically secure.
- Personal or sensitive data should not be stored on the local drives of desktop PC, laptop, USB memory stick or other portable device. If it is necessary to do so the local drive must be 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 any unauthorised person.
- All ICT equipment allocated to staff must be authorised by the Deputy Headteacher or School Business Manager.

23.2 New technological devices

New personal technological devices may offer opportunities for teaching and learning. However, the school must consider educational benefit and carry out risk assessment before use in school is allowed. Parents/carers, pupils and staff should not assume that new technological devices will be allowed in school and should check with Roz Torres or Natalie Phillips before they are brought into school.

23.3 Use of personal mobile devices (including phones)

The school allows staff, including temporary and peripatetic staff, and visitors to use personal mobile phones and devices only in designated areas and never in the presence of pupils. The school requests that staff members do not contact parents/carers using their personal device, where it is absolutely necessary that they do staff members are required to withhold their number when calling.

Parents/carers may only use personal mobile phones and devices in designated areas unless otherwise informed, e.g. for specific events and activities. Under no circumstance should images be taken at any time on school premises or on off-site school events and activities of anyone other than their own child, unless there is a pre-specified permission from the Headteacher. When a parent/carer is on school premises but not in a designated area, their phone/s must be switched off and out of sight.

Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

Personal mobiles must never be used to access school data. The only exception would be where a closed, monitored system has been set up by the school for use on a personal device.

23.3.1 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.

24. Telephone Services

- You may make or receive personal telephone calls provided:
    - They are infrequent, kept as brief as possible and do not cause annoyance to others.
    - They are not for profit or to premium rate services.

- They conform to this and other relevant HCC and school policies.

- School telephones are provided specifically for school business purposes and personal usage is a privilege that will be withdrawn if abused.
- Be aware that the laws of slander apply to telephone calls. Whilst a telephone call may seem to have a temporary and private existence it still qualifies as admissible evidence in slander law cases.
- Ensure that your incoming telephone calls can be handled at all times.
- Follow the appropriate procedures in the event of receiving a telephone call containing a bomb threat. These procedures should be made readily available throughout your office. If you do not have a copy, please ask the School Business Manager.

25. Servers

- Always keep servers in a locked and secure environment.
- Limit access rights.
- Always password protect and lock the server.
- Existing servers should have security software installed appropriate to the machine's specification.
- Data must be backed up regularly to the cloud server.

26. Social Media, including Facebook and Twitter

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

- Staff *are not* permitted to access their personal social media accounts using school equipment whilst at school.
- Staff, governors, pupils, 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, pupils, parents and carers are aware that their online behaviour should at all times be compatible with UK law.

27. Policy review Procedure

- This policy will be reviewed every 24 months and consideration will be given to practises in school and 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.

28. Further Help and Support

If you require further advice on eSafety issues please visit the school website.

If you require further advice on GDPR please visit ico.org.uk

Appendix 1

ICT Acceptable Use Agreement – Pupils

Tannery Drift
First School
ROYSTON • HERTFORDSHIRE
www.tannerydrift.herts.sch.uk

- ✓ I will only use school ICT for school purposes agreed by school staff.
- ✓ I will only use my class email address or my own school email address when emailing.
- ✓ I will not sign up for any online service on school devices or school platforms unless this has been approved by my teacher.
- ✓ I will only open email attachments when it has been approved by a member of school staff in school or a parent/carer out of school.
- ✓ I will only open, edit or delete my own school files.
- ✓ I will not tell anyone other than my parents/carers my passwords. I will not use other people's usernames or passwords to pretend to be them online.
- ✓ I will make sure that all online contact that I make is responsible, polite and sensible. I will be kind and respectful at all times.
- ✓ I will not deliberately look for, save or send anything upsetting, unpleasant or nasty. If I accidently find anything like this, or that makes me feel unsafe, I will tell my teacher or my parent/carer immediately.
- ✓ If someone says, asks or posts about me anything upsetting, unpleasant or nasty, or anything that makes me feel unsafe, I will not reply. I will tell my teacher or my parent/carer immediately.
- ✓ I will not give out my own or others' personal information, including: name, phone number, home address, interests, schools or clubs or any personal image. I will tell my teacher or parent/carer if anyone asks me online for personal information.
- ✓ I understand that some people on the internet are not who they say they are and some people are not safe to be in contact with. I will not arrange to meet someone I only know on the internet. If someone asks to meet me, I will not reply to them and I will tell a teacher or a parent/carer immediately.
- ✓ Uploading or sending my image online puts me at risk. I will always seek permission from my teacher or parent/carer if I wish to do this. I will not take, share or upload any image of anyone else without their permission and also, if they are a child, without their parents'/carers' permission.
- ✓ Even with their permission, I will not upload any images, videos, sounds or words that could upset, now or in the future, any member of the school community.
- ✓ I understand that everything I do or receive online can be traced now and in the future.
- ✓ I understand that school staff have the right to access anything I create and use on school ICT equipment or platforms, including monitoring websites I visit. I know that my use of ICT can be checked and that my parent/ carer will be contacted if a member of school staff is concerned about my eSafety.
- ✓ I understand that these rules are designed to keep me safe now.

Appendix 2

ICT Acceptable Use Agreement: Parents/Carers

Tannery Drift
First School
ROYSTON · HERTFORDSHIRE
www.tannerydrift.herts.sch.uk

- ✓ I will support the school's approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community on any internet media, such as Facebook, Twitter etc.
- ✓ I understand that it is my responsibility to monitor what my child accesses online at home.
- ✓ I agree only to use personal mobile phones and devices in designated areas of the school unless otherwise informed, e.g. for specific events and activities. I understand that under no circumstance should images be taken at any time on school premises that include anyone other than my own child, unless there is a pre-specified agreement with individuals and parents/carers. When I am on the school premises and not in a designated area, my phone/s must be silenced and out of sight.
- ✓ I understand that the school will investigate and respond to all reported cyberbullying incidents and eSafety breaches. No reply should ever be sent to the sender/poster of cyberbullying content. Evidence should be retained and shown in school. Evidence should not be forwarded.
- ✓ I acknowledge that the school reserves the right to access content that my child saves on any school platform, including for monitoring purposes.
- ✓ I acknowledge that I do not have the right to set up any site, page, chat group or any other online presence that uses the school name or logo in any form.
- ✓ If understand that if I feel distressed or concerned about an aspect of school I should make immediate contact with an appropriate member of staff rather than posting my concern online. I must not post or share school related information, images or material online that may bring the school or any individual within it into disrepute (parents/carers are encouraged to report breaches so that we can protect the reputation of the school, staff, pupils and parents/carers).
- ✓ I understand that the school will take all reasonable precautions to ensure pupils cannot access inappropriate materials and that the school cannot be held responsible for the nature or content of materials accessed through the internet.
- ✓ I have supported my child to understand and sign the Online Safety Acceptable Use Agreement for pupils and will ensure my child will abide by the school rules with regard to internet safety.

Parent(s)/Carer(s) agreement	Pupil agreement
Parent(s)/Carer(s) name(s)	Pupil name
.....	.....
Parent/carer signature(s)	Pupil signature
.....	.....

Appendix 3

Online Safety Acceptable Use Agreement - Staff, Governors and student teachers (on placement or on staff)

You must read this agreement in conjunction with the online safety policy and the GDPR policy. Once you have read these, you must sign and submit this agreement and it will be kept on record in the school. You should retain your own copy for reference. This forms part of your professional and safeguarding responsibilities.

Internet, mobile and digital technologies are part of our daily working life and this agreement is designed to ensure that all staff and governors are aware of their responsibilities in relation to their use. All staff, student teachers and governors are expected to adhere to this agreement and to the online safety policy. Any concerns or clarification should be discussed with
Anna Greetham. Breaches will be investigated, recorded and, where appropriate, disciplinary procedures will apply and police involvement will be sought.

Internet Access

I will not access or attempt to access any sites that contain any of the following: child abuse; pornography; discrimination of any kind; promotion of prejudice against any group; promotion of illegal acts; any other information which may be illegal or offensive. Inadvertent access on school equipment must be treated as an online safety incident, reported to the online safety lead and/or DSP and an incident report completed.

Online conduct

I will ensure that my online activity, both in and outside school, will not bring the school, my professional reputation, or that of others, into disrepute.

I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory. Exceptionally, use of controversial material as part of the curriculum should be planned and approved on every occasion (see policy).

I will report any accidental access to or receipt of inappropriate materials or filtering breach to Anna Greetham.

I understand that all my use of the internet and other related technologies can be traced and monitored and, should it be required, must be made available to my line manager, Headteacher and others as required.

I will not give out my personal contact and online account information such as phone numbers, email address, and social media account details to pupils and/or parents/carers.

Social networking

I understand the need to separate my professional role from my private friendships; in my professional capacity I will not become 'friends' with parents/carers or pupils on social networks. Where my school role is my only connection to an individual, private online contact is unacceptable with parents/carers or pupils.

When using social networking for personal use I will ensure my settings are not public. My private account postings will never undermine or disparage the school, its staff, governors, parents/carers or pupils. Privileged information must remain confidential.

I will not upload any material about or references to the school or its community on my personal social networks.

Passwords

I understand that there is no occasion when a password should be shared with a pupil or anyone who is not a staff member.

Data protection

I will follow requirements for data protection as outlined in GDPR policy. These include:

- Photographs must be kept securely and used appropriately, whether in school, taken off the school premises or accessed remotely
- Personal data can only be taken out of school or accessed remotely when authorised by the Headteacher or governing body
- Personal or sensitive data taken off site must be encrypted

Images and videos

I will only upload images or videos of staff, pupils or parents/carers onto school approved sites where specific permission has been granted.

I will not take images, sound recordings or videos of school events or activities on any personal device.

Use of email

I will use my school email address or GovernorHub for all school business. All such correspondence must be kept professional and is open to Subject Access Requests under the Freedom of Information Act. I will not use my school email addresses or GovernorHub for personal matters or non-school business.

Use of personal devices

I understand that as a member of staff I should at no time put myself in a position where a safeguarding allegation can be made against me as a result of my use of personal devices. I understand that the use of personal devices in school is at the discretion of the Headteacher.

I will only use approved personal devices in designated areas and never in front of pupils.

I will not access secure school information from personal devices when in school or any other location unless using LARA, a closed, monitorable system used by the school. LARA ensures as the user I am not saving files locally to my own device and breaching data security.

Through LARA, any school documents accessed on a personal device are never actually on the computer being used, they remain on the school server. When the user logs-out of LARA, there are no copies left on their own device.

Additional hardware/software

I will not install any hardware or software on school equipment without permission of Roz Torres or Natalie Phillips.

Promoting online safety

I understand that online safety is the responsibility of all staff and governors and I will promote positive online safety messages at all times including when setting homework or providing pastoral support.

I understand that it is my duty to support a whole school safeguarding approach and will report any inappropriate or concerning behaviour (of other staff, governors, visitors, pupils or parents/carers) to the DSP.

Classroom management of internet access

I will check for appropriateness all internet sites used in the classroom this will include the acceptability of other material visible, however briefly, on the site. I will not free-surf the internet in front of pupils. I will also check the suitability of any suggested sites suggested for home learning, as appropriate to my role.

Video conferencing

I will only use the conferencing tools that have been identified and risk assessed by the school leadership, DPO and DSP. A school-owned device should be used by school staff when running video-conferences, where possible.

User signature

I agree to follow this Acceptable Use Agreement and to support online safety throughout the school. I understand this forms part of the terms and conditions set out in my contract of employment (staff members only) and/or my responsibilities as a governor.

Signature ..... Date .....

Full Name ..... (printed)

Job title .....

Appendix 4

Online Safety Acceptable Use Agreement - Peripatetic teachers/coaches, supply teachers

Tannery Drift First School

Designated Safeguarding Lead (DSP) – Anna Greetham (DSP), Roz Torres (Deputy DSP), Beth Robins (Deputy DSP), Beth Kerr (Deputy DSP)

This agreement forms part of your professional and safeguarding responsibility in the school. You must read and sign this agreement. This will be kept on record and you should retain your own copy for reference.

Internet, mobile and digital technologies are part of our daily working life and this agreement is designed to ensure that all staff and governors are aware of their responsibilities in relation to their use. You are expected to adhere to this agreement. Any concerns or clarification should be discussed with the Headteacher. Breaches will be investigated, recorded and, where appropriate, disciplinary procedures will apply and police involvement will be sought.

The school's online safety policy will provide further detailed information as required.

Internet Access

I will not access or attempt to access any sites that contain any of the following: child abuse; pornography; discrimination of any kind; promotion of prejudice against any group; promotion of illegal acts; any other information which may be illegal or offensive. Inadvertent access on school equipment must be treated as an online safety incident, reported to the DSP and an incident report completed.

Online conduct

I will ensure that my online activity, both in and outside school, will not bring the school, my professional reputation, or that of others, into disrepute.

I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory. Exceptionally, use of controversial material as part of the curriculum should be planned and approved on every occasion (see policy).

I will report any accidental access to or receipt of inappropriate materials or filtering breach to the Headteacher.

I understand that all my use of the internet and other related technologies can be traced and monitored and, should it be required, must be made available to my line manager, Headteacher and others as required.

I will not give out my personal contact and online account information such as phone numbers, email address, and social media account details to pupils and/or parents/carers.

Should I need to share my professional details, such as mobile phone number or email address, with parent/carers, this must be agreed in advance as an acceptable approach with the Headteacher.

Social networking

I understand the need to separate my professional role from my private friendships; in my professional capacity I will not become 'friends' with parents/carers or pupils on social networks. Where my school role is my only connection to an individual, private online contact is unacceptable with parents/carers or pupils.

Information can be shared with pupils over 13 and parents/carers through an organisational social network site/page e.g. on Facebook or Twitter, but never through a personal account or site. In my professional role in the school, I will never engage in 1-1 exchanges with pupils or parent/carers on personal social network sites.

My private account postings will never undermine or disparage the school, its staff, governors, parents/carers or pupils. Privileged information known as a result of my work in the school must remain confidential.

I will not upload any material about or references to the school or its community on my personal social networks.

Passwords

I must clarify what access I may have to the internet and/or school systems. If I have access of any kind, I understand that there is no occasion when a password should be shared with a pupil or anyone who is not a staff member.

Data protection

I will follow all requirements for data protection explained to me by the school. These include:

- I must consult with the school before making any recordings, photographs and videos. Once agreed, these must be made on a school device.
- I understand that there are strict controls and requirements regarding the collection and use of personal data. I will follow all requirements regarding GDPR.

Images and videos

I will only upload images or videos of staff, pupils or parents/carers onto school approved sites where specific permission has been granted.

I will not take images, sound recordings or videos of tuition or wider school activities on any personal device. School devices can be used for this purpose.

Internet, mobile and digital technologies provide helpful recording functions but these cannot be made on a teacher's personal device. Recordings can be made with the child's and parent/carer's agreement on a school device or an organisational device approved by the Headteacher.

Use of Email

I will only use my professional email address for all school business. All such correspondence should be kept professional and is open to Subject Access Requests under the Freedom of Information Act. I will not use my professional email addresses for personal matters.

Use of personal devices

I understand that when working in the school I should at no time put myself in a position where a safeguarding allegation can be made against me as a result of my use of personal devices. I understand that the use of personal devices in school is at the discretion of the Headteacher.

I will only use approved personal devices in designated areas and never in front of pupils. This therefore precludes use of specialist apps on personal devices. A school device could be used to access specialist apps that support pupil learning.

Additional hardware/software

I will not install any hardware or software on school equipment without permission of Roz Torres or Natalie Phillips.

Promoting online safety

I understand that online safety is part of my responsibility and I will promote positive online safety messages at all times, including when setting homework, rehearsal or skill practice or when providing pastoral support.

I understand that it is my duty to support a whole school safeguarding approach and will report any behaviour (of staff, governors, visitors, pupils or parents/carers) which I believe may be inappropriate or concerning in any way to the DSP.

Classroom management of internet access

I will check for appropriateness all internet sites used in the classroom or during a tutoring session; this will include the acceptability of other material visible, however briefly, on the site. I will not free-surf the internet in front of pupils.

Video conferencing

I will only use the conferencing tools that have been identified and risk assessed by the school leadership, DPO and DSP. A school-owned device should be used when running video-conferences, where possible.

User Signature

I agree to follow this Acceptable Use Agreement and to support online safety in my work in the school. I understand this forms part of my company/educational setting/organisation's contract with the school.

Signature ..... Date .....

Full Name ..... (Please use block capitals)

Job Title/Role .....

Appendix 5

Requirements for visitors, volunteers and parent/carer helpers (Working directly with children or otherwise)

Tannery Drift First School

Designated Safeguarding Lead (DSP) – Anna Greetham (DSP), Roz Torres (Deputy DSP), Beth Robins (Deputy DSP), Beth Kerr (Deputy DSP)

This document is designed to ensure that you are aware of your responsibilities when using any form of IT in the school and other aspects of safeguarding in connection with online safety.

Please raise **any** safeguarding concerns arising from your visit immediately with the DSP.

- I understand I may only use my personal mobile phone(s) and other devices with camera functions in designated areas. When not in a designated area, phones must be switched off and out of sight. Any exception must be pre-arranged.
- I will not take images, sound recording or videos of school events or activities, on or off site, on any device. Any possible exception must be pre-arranged.
- I will not give out my personal details such as mobile phone number, email address, and social media account details to pupils. Where appropriate I may share my professional contact details with parents/carers provided the DSP or Headteacher is informed before I leave the school.
- I understand my visit to the school may give me access to privileged information about pupils, staff, school systems and plans. Such information should never be shared on line, including on social media sites.
- I understand I should not use school equipment to access the internet without prior approval from my contact in the school or the Headteacher.
- If working in the classroom, I will pre-check for appropriateness all internet sites I intend to use including checking the acceptability of other material visible on the site. I will not free-surf the internet in front of pupils. If I am in any doubt about the appropriateness of the content I plan to use I will check with my contact in the school.

Signature ..... Date .....

Full Name ..... (Please use block capitals)

Appendix 6

Online safety policy guide - Summary of key parent/carer responsibilities

The school provides online safety information for parents/carers, through the website, in newsletters and at events. It is important that parents/carers understand their key role in supporting children to behave appropriately and keep themselves safe online.

The online safety policy, supported by its acceptable use agreements, is intended to protect the interests and safety of the whole school community.

- Parents/carers are required to support their child in understanding and signing the Online Safety Acceptable Use Agreement for pupils.

- Parents/carers may only use personal mobile phones and devices in designated areas of the school unless otherwise informed, e.g. for specific events and activities. Under no circumstance should images be taken at any time on school premises that include anyone other than their own child, unless there is a pre-specified agreement with individuals and parents/carers. When a parent/carer is on school premises but not in a designated area, their phone/s must be switched off and out of sight.

- Parents/carers should not assume that pupils can bring technological devices to school and should always check the school policy.

- All cyberbullying incidents affecting children in the school should be reported immediately. (If the incident involves an indecent image of a child the report must also be made immediately to the police for your own protection.) The school will investigate and respond to all reported cyberbullying incidents, liaising with others where appropriate. No reply should ever be sent to the sender/poster of cyberbullying content. If applicable block the sender and report abuse to the site. Evidence should be retained and shown in school and/or to the police. Evidence should not be forwarded.

- The school may choose to set up social media sites, blogs or have some other online presence in its own name. Parents/carers, however, do not have the right to set up any site, page, chat group or any other online presence that uses the school name or logo in any form.

- Any parent/carer, distressed or concerned about an aspect of school should make immediate contact with a member of staff rather than posting their concerns online. Parents/carers should not share school related information or images online or post material that may bring the school or any individual within it into disrepute. Negative postings about the school would impact on the reputation of the whole school community. Parents/carers are encouraged to report breaches so that we can protect the reputation of the school, staff, pupils and parents/carers.

Please see the full online safety policy in the policies section on the school website.

Appendix 7

Guidance on the process for responding to cyberbullying incidents

All cyberbullying incidents should be reported and responded to. Where the perpetrator is a member of the school community the majority of cases can be dealt with through mediation and/or disciplinary processes.

The following procedures are recommended:

- Never reply to the sender/poster of cyberbullying content. If applicable, block the sender.
- Incidents should be reported immediately. Pupils should report to a member of staff (e.g. class teacher, Headteacher) and staff members should seek support from their line manager or a senior member of staff.
- The person reporting the cyberbullying should save the evidence and record the time and date. This evidence must not be forwarded but must be available to show at a meeting. Under no circumstances should indecent images of children and young people be printed or forwarded as this is a further criminal act. Staff should not ask to see the evidence of reported indecent images of children or young people but must refer this immediately to the police. Any member of staff being shown such evidence should immediately inform their line manager or the Headteacher so that the circumstances can be recorded.
- A senior member of staff will meet with the person who has reported the incident and the target, if different, to listen, reassure and support. All relevant facts will be reviewed and documented.
- A senior member of staff will conduct an investigation.
- Anyone found to have cyberbullied will have attention drawn to the seriousness of their behaviour and if necessary the police will be involved. If the comments are threatening, abusive, sexist, of a sexual nature, constitute a hate crime or are libellous they may well break the law. Online harassment and stalking is also a crime.
- Once evidence has been secured then the person who has cyberbullied will be requested to remove the offending comments/material. Any refusal will lead to an escalation of sanctions.

Appendix 8

Guidance for staff on preventing and responding to negative comments on social media

The school should make it clear which, if any, social media platforms are used to communicate with parents/carers. If used correctly, parents can use a school's social media site as a source of reliable information. The online safety policy, clarifies that no other social media platforms should be set up using the school's name or logo.

The school should regularly reinforce with all parties that discussion of school issues on social media platforms, either positive or negative, should not take place as this could bring the school into disrepute and affect families and children. Parents should be encouraged to be good online role models and not post statements written in anger or frustration. Identified routes to raise concerns directly with the school should be used.

If negative comments are posted, collect the facts

As soon as you become aware of adverse comments relating to the school you need to establish what is being said. It is essential that if you have access to the postings they are secured and retained together with any other evidence. Do not become engaged in responding directly.

If the allegations against a member of staff or a pupil are of a serious nature, these will need to be formally investigated. This may involve the police and the Headteacher will need to follow the school's safeguarding procedures.

If there is a risk of serious damage to the school reputation or the reputation of individual members of staff, professional legal advice should be sought.

Adverse comments of any kind are highly demotivating and cause stress and anxiety. It is important that the senior staff reassure and support all staff and/or other affected members of the school community.

Addressing negative comments and complaints

Contact the complainants and invite them to a meeting. In the meeting, make sure you have any evidence available. The meeting must:

- Draw attention to the seriousness and impact of the actions/postings;
- Ask for the offending remarks to be removed;
- Explore the complainant's grievance;
- Agree next steps;
- Clarify the correct complaints procedures.

If the meeting does not resolve the issue, the parents must be informed that the school will need to take the matter further. This may include:

- Reporting the matter to the social network site if it breaches their rules or breaks the law;
- Reporting the matter to the police if it breaks the law, e.g. if the comments are threatening, abusive, malicious, sexist, of a sexual nature, constitute a hate crime or are libellous they may well break the law. Online harassment and stalking is also a crime.

If inappropriate postings continue or the original material is not removed, a second meeting is advisable to re-iterate the seriousness of the matter.

Appendix 9

Online safety incident reporting form

Any member of the school community can raise a concern about an online safety incident. If you have witnessed or experienced an incident please complete the form below to help us to address the issue. It is important that you provide as much detail as possible. Once completed please hand this report to a DSP or Deputy DSP, alternatively please log all details on CPOMS (Child Protection Online Management System) and alert the DSP and Deputy DSPs.

Name of person reporting incident:				
Signature:				
Date you are completing this form:				
Where did the incident take place:	Inside school?		Outside school?	
Date of incident(s):				
Time of incident(s):				
Who was involved in the incident(s)?	Full names and/or contact details			
Children/young people				
Staff member(s)				
Parent(s)/carer(s)				
Other, please specify				

Type of incident(s) (indicate as many as apply)			
Accessing age inappropriate websites, apps and social media		Accessing someone else's account without permission	
Forwarding/spreading chain messages or threatening material		Posting images without permission of all involved	
Online bullying or harassment (cyber bullying)		Posting material that will bring an individual or the school into disrepute	
Racist, sexist, homophobic, religious or other hate material		Online gambling	
Sexting/Child abuse images		Deliberately bypassing security	
Grooming		Hacking or spreading viruses	
Accessing, sharing or creating pornographic images and media		Accessing and/or sharing terrorist material	
Accessing, sharing or creating violent images and media		Drug/bomb making material	
Creating an account in someone else's name to bring them into disrepute		Breaching copyright regulations	
Other breach of acceptable use agreement, please specify			

Full description of the incident	What, when, where, how?
Name all social media involved	Specify: Twitter, Facebook, Whatsapp, Snapchat, Instagram etc
Evidence of the incident	Specify any evidence available but do not attach.

Appendix 10

Online safety incident record

Name of person reporting incident:				
Date of report:				
Where did the incident take place:	Inside school?		Outside school?	
Date of incident(s):				
Time of incident(s):				
Who was involved in the incident(s)?	Full names and/or contact details			
Children/young person				
Staff member(s)				
Parent(s)/carer(s)				
Other, please specify				

Type of incident(s) (indicate as many as apply)			
Accessing age inappropriate websites, apps and social media		Accessing someone else's account without permission	
Forwarding/spreading chain messages or threatening material		Posting images without permission of all involved	
Online bullying or harassment (cyberbullying)		Posting material that will bring an individual or the school into disrepute	
Racist, sexist, homophobic, religious or other hate material		Online gambling	
Sexting/Child abuse images		Deliberately bypassing security	
Grooming		Hacking or spreading viruses	
Accessing, sharing or creating pornographic images and media		Accessing and/or sharing terrorist material	
Accessing, sharing or creating violent images and media		Drug/bomb making material	
Creating an account in someone else's name to bring them into disrepute		Breaching copyright regulations	
Other breach of Acceptable Use Agreement			
Other, please specify			

Full description of the incident	What, when, where, how?
Name all social media involved	Specify: Twitter, Facebook, Whatsapp, Snapchat, Instagram etc
Evidence of the incident	Specify any evidence provided but do not attach

Immediate action taken following the reported incident:	
Incident reported to DSP/Headteacher	
Safeguarding advice sought, please specify	
Referral made to HCC Safeguarding	
Incident reported to police and/or CEOP	
Online safety policy to be reviewed/amended	
Parent(s)/carer(s) informed please specify	
Incident reported to social networking site	
Other actions e.g. warnings, sanctions, debrief and support	
Response in the wider community e.g. letters, newsletter item, assembly, curriculum delivery	

Brief summary of incident, investigation and outcome (for monitoring purposes)	

Appendix 11

Online safety incident log

Summary details of ALL online safety incidents will be recorded on this form by the designated member of staff. This incident log will be monitored at least termly and information reported to SLT and governors.

Date & time	Name of pupil or staff member Indicate target (T) or offender (O)	Nature of incident(s)	Details of incident (including evidence)	Outcome including action taken

Appendix 12

Safeguarding and remote education during coronavirus (COVID-19)

Useful resources

Below are resources (please note not an exhaustive list) to help schools manage and risk assess any remote teaching and working.

Government guidance on safeguarding and remote education
https://www.gov.uk/guidance/safeguarding-and-remote-education-during-coronavirus-covid-19

The Key for School Leaders - Remote learning: safeguarding pupils and staff
https://schoolleaders.thekeysupport.com/covid-19/safeguard-and-support-pupils/safeguarding-while-teaching/remote-teaching-safeguarding-pupils-and-staff/?marker=content-body

NSPCC Undertaking remote teaching safely
https://learning.nspcc.org.uk/news/2020/march/undertaking-remote-teaching-safely

LGfL Twenty safeguarding considerations for lesson livestreaming
https://static.lgfl.net/LgflNet/downloads/digisafe/Safe-Lessons-by-Video-and-Livestream.pdf

swgfl Remote working a guide for professionals
https://swgfl.org.uk/assets/documents/educational-professionals-remote-working.pdf

National Cyber Security Centre Video conferencing. Using services securely
https://www.ncsc.gov.uk/files/vtc_infographic.pdf

Tannery Drift
First School

Tannery Drift - Royston - Hertfordshire - SG8 5DE

01763 246549 admin@tannerydrift.herts.sch.uk
www.tannerydrift.herts.sch.uk

Enjoyment – Achievement – Respect