Online Safety Policy

The Vyne Community School

Approved at:	C&S Committee	Date: 3rd February 2026
Last reviewed on:	February 2026	
Next review due by:	February 2027	

Linked Policies/Documents:
Child Protection Policy
Safeguarding Policy
Social Media Policy
Behaviour Management
Anti-Bullying
Prevent Strategy
Searching, Screening and Confiscation Policy
Managing Allegations against Students Policy
Acceptable Use Agreement of ICT for Staff
Computer Systems and Internet Agreement for Students
Acceptable User Policy (Annex 2)
Staff Behaviour Code of Conduct

This policy is part of The Vyne Community School's Statutory Safeguarding Procedures and Policy. Any issues and concerns with online safety must follow the school's safeguarding and child protection processes.

CONTENTS

1. Introduction and Overview
   - Rationale and Scope
   - Roles and responsibilities
   - How the policy is communicated to staff/students/community
   - Handling complaints
   - Reviewing and Monitoring

2. Education and Curriculum
   - Student online safety curriculum
   - Staff and governor training
   - Parent awareness and training

3. Expected Conduct and Incident Management
   - Expected Conduct
   - Staff, Volunteers and Contractors
   - Parents/Carers
   - Incident Management

4. Managing the IT Infrastructure
   - Internet access, security (virus protection) and filtering
   - Network management (user access, backup, curriculum and admin)
   - Passwords policy
   - E-mail
   - School website
   - Learning platform
   - Social networking
   - CCTV

5. Data Security
   - Management Information System access
   - Data transfer
   - Asset Disposal

6. Equipment and Digital Content
   - Personal mobile phones and devices
   - Digital images and video

1. INTRODUCTION AND OVERVIEW

1.1 RATIONALE

All schools must have regards to 'Keeping Children Safe in Education' (September 2022) when carrying out their duties to safeguard and promote the welfare of children. At The Vyne Community School staff, students, parents/carers and governors recognise that they exist in a world where technology is readily available to all. The school embraces the impact that such technology can have on a young person's social development, employability and technological competency. In addition, we recognise how a child's learning can be enriched by access to a range of learning resources.

The Vyne Community School takes very seriously its responsibility for the 'Online Safety' of its community. We recognise that the abuse of technology, including malicious use of social media and the Internet, can have profound psychological and material consequences for targets of such abuse and therefore make every effort to ensure that safe use of technology is ensured within and outside of school.

WHAT IS ONLINE SAFETY?

Online Safety encompasses internet technologies and electronic communications such as mobile phones and wireless technology. It highlights the need to educate young people and parents/carers about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experiences.

The Schools' Online Safety Policy has been written to reflect the need to raise awareness of the safety issues associated with electronic communications as a whole. It must be read in conjunction with the school's Website Policy.

The purpose of this policy is to:

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

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

CONTENT

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

CONTACT

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

CONDUCT

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

1.2 SCOPE

This Online Safety Policy outlines the commitment of the Vyne school to safeguard members of our school community online in accordance with statutory guidance and best practice.
This Online Safety Policy applies to all members of the school community (including staff, learners, governors, volunteers, parents and carers, visitors, community users) who have access to and are users of school digital systems, both in and out of the school. It also applies to the use of personal digital technology on the school site (where allowed).
Vyne school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that take place out of school.

Roles and responsibilities

Role	Key Responsibilities
Headteacher	● Must be adequately trained in off-line and online safeguarding, in-line with statutory guidance and relevant Local Safeguarding Children Board (LSCB) guidance ● To lead a 'safeguarding' culture, ensuring that online safety is fully integrated with whole school safeguarding. ● To take overall responsibility for online safety provision ● To take overall responsibility for data management and information security (SIRO) ensuring school's provision follows best practice in information handling ● To ensure the school uses appropriate IT systems and services including, filtered Internet Service and Hampshire County Council services ● To be responsible for ensuring that all staff receive suitable training to carry out their safeguarding and online safety roles ● To be aware of procedures to be followed in the event of a serious online safety incident ● Ensure suitable 'risk assessments' undertaken so the curriculum meets needs of students, including risk of children being radicalised ● To receive regular monitoring reports from the Designated Safeguarding Lead ● To ensure that there is a system in place to monitor and support staff who carry out internal online safety procedures, e.g. network manager ● To ensure Governors are regularly updated on the nature and effectiveness of the school's arrangements for online safety ● To ensure the school website includes relevant information.
Online Safety Lead	● Act as a named point of contact on all online safeguarding issues and liaising with other members of staff and other agencies as appropriate. ● Keep up-to-date with current research, legislation and trends regarding online safety. ● Coordinate participation in local and national events to promote positive online behaviour, e.g. Safer Internet Day. ● Ensure that online safety is promoted to parents and carers and the wider community through a variety of channels and approaches. ● Work with the school/setting lead for data protection and data security to ensure that practice is in line with current legislation. ● Maintain a record of online safety concerns/incidents and actions taken as part of the schools safeguarding recording structures and mechanisms. ● Monitor the school/settings online safety incidents to identify gaps/trends and use this data to update the school/settings education response to reflect need ● report to the school management team, Governing Body and other agencies as appropriate, on online safety concerns and local data/figures. ● Liaise with the local authority and other local and national bodies, as appropriate. ● Work with the school/setting leadership and management to review and update the online safety policies, Acceptable Use Policies (AUPs) and other related policies on a regular basis (at least annually) with stakeholder input. ● Ensure that online safety is integrated with other appropriate school policies and procedures.
Safeguarding Governor	● To ensure that the school has in place policies and practices to keep the children and staff safe online

(including online safety)	● To approve (via committee) the Online Safety Policy and review the effectiveness of the policy ● To support the school in encouraging parents and the wider community to become engaged in online safety activities ● The role of the Safeguarding Governor will include: regular review with the Designated Safeguarding Lead (Online Safety Lead).

Computing Subject Leader	● To oversee the planning, delivery and impact of the online safety element of the Computing curriculum
Network Manager	● Work closely with the school leaders, Designated Safeguarding Lead safeguarding lead as well as pastoral and curriculum staff (where appropriate) to provide expertise relating to appropriate education use of ICT systems and also to ensure that learning opportunities are not unnecessarily restricted by technical safety measures. ● Be clear about the procedures they must follow if they discover, or suspect, online safety incidents through monitoring of network activity and the need for these issues to be escalated immediately to the Designated Safeguarding Lead/Headteacher with existing school safeguarding policies. ● Ensure that an external service provider upholds the online safety practices including referring any concerns to the online safety coordinator or senior leadership team. ● Ensure that the school network is monitored and any concerns reported to the Designated Safeguarding Lead ● Develop an understanding of the relevant legislation ● Ensure that the school's ICT infrastructure is secure but not so secure that it gets in the way of learning. ● Ensure that appropriate anti-virus software and system updates are installed and maintained on all electronic devices. ● To manage the school's computer systems, ensuring - school password policy is strictly adhered to. - systems are in place for misuse detection and malicious attack (e.g. keeping virus protection up to date) - access controls/encryption exist to protect personal and sensitive information held on school-owned devices - the school's policy on web filtering is applied and updated on a regular basis ● That they keep up to date with the school's Online Safety policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant ● To ensure appropriate backup procedures and disaster recovery plans are in place ● To keep up-to-date documentation of the school's online security and technical procedures
Data and Information (Asset Owners) Managers (IAOs)	● To ensure that the data they manage is accurate and up-to-date ● Ensure best practice in information management. i.e. have appropriate access controls in place, that data is used, transferred and deleted in-line with data protection requirements. ● The school is registered with Information Commissioner

Teaching Staff	● Contributing to the development of online safety policies ● Reading and adhering to Acceptable Use Policies (AUPs) ● Taking responsibility for the security of school/ setting systems and data ● Having an awareness of a range of different online safety and how they relate to safeguarding children. This should include sexting and cyberbullying. ● Modelling good practice when using new and emerging technologies ● Embedding online safety education in curriculum delivery wherever possible ● Identifying individuals of concern and taking appropriate action by following school safeguarding policies and procedures ● Knowing when and how to escalate online safety issues, internally and externally ● Maintain a professional level of conduct in their personal use of technology, both on and off site. ● Taking personal responsibility for professional development in this area.
All staff, volunteers and contractors.	● To read, understand, sign and adhere to the school staff Acceptable Use of ICT Agreement/Policy, and understand any updates annually. This is also signed by new staff on induction. ● To report any suspected misuse or problem to the Designated Safeguarding Lead (Online Safety Lead). ● To maintain an awareness of current online safety issues and guidance e.g. through CPD, staff briefings, regular email updates. ● To model safe, responsible and professional behaviours in their own use of technology **Exit strategy** ● At the end of the period of employment/volunteering to return any equipment or devices loaned by the school. This will include leaving PINs, IDs and passwords to allow devices to be reset, or meeting with line manager and technician on the last day to login and allow a factory reset.
Students	● Contribute to the development of these policies ● Read, understand, sign and adhere to the Computer Systems and Internet Agreement (example Annex 1) on entry to the school ● Respect the feelings and right of others both online and offline ● Seek help from a trusted adult if things go wrong, and supporting others that may be experiencing online safety issues ● Take responsibility for understanding risks posed by new technologies ● Assess the personal risk of using any particular technology and behave safely and responsibly to limit those risks ● To understand the importance of reporting abuse, misuse or access to inappropriate materials ● To be aware of the Child Exploitation and Online Protection (CEOP) reporting abuse mechanism via the school website. ● To know what action to take if they or someone they know feels worried or vulnerable when using online technology ● To understand the importance of adopting safe behaviours and good online safety practice when using digital technologies out of school and realise that the school's Online Safety policy covers their actions out of school ● To contribute to any 'student voice' / surveys that gathers information of their online experiences

Parents/ Carers	● Read the school AUP, encourage themselves and their children to adhere to them ● Discuss online safety issues with their children, supporting the school in their online safety approaches, and reinforcing appropriate safe online behaviours at home. ● Role model safe and appropriate uses of technology and social media. ● Identify changes in behaviour that could indicate that their child is at risk of harm online. ● Seek help and support from the school, or other appropriate agencies, if they or their child encounters online problems or concerns. ● to support the school in promoting online safety and endorse the school's internet safety procedures and the school's use of photographic and video images.
External groups including Parent Groups	● To support the school in promoting online safety ● To model safe, responsible and positive behaviours in their own use of technology.

1.3 COMMUNICATION

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

- Policy to be posted on the school website and school computer system.
- Policy to be part of the school induction pack for new staff.
- Regular updates and training on online safety for all staff.
- Acceptable use agreements discussed with staff.
- Students sign Computer Systems and Internet Agreement on entry to school.
- Acceptable use agreements to be issued to the whole school community, on entry to the school.

1.4 HANDLING INCIDENTS

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

1.5 REVIEW AND MONITORING

The Online Safety policy is linked with other school policies (e.g. Child Protection Policy, Safeguarding policy, Anti-Bullying policy, Behaviour Management, Prevent).

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

2. EDUCATION AND CURRICULUM

2.1 STUDENT ONLINE SAFETY CURRICULUM

This school:

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

2.2 STAFF TRAINING

This school:

- Makes regular training available to staff on online safety issues and the school's online safety education program;
- Provides, as part of the induction process, all new staff [including those on university/college placement and work experience] with information and guidance on the Online Safety Policy and the school's Acceptable Use Agreement.

2.3 PARENT AWARENESS AND TRAINING

The school will take every opportunity to help parents and carers understand these issues through:

- Publishing the school Online Safety Policy on the school website
- Providing them with a copy of the learners' acceptable use agreement
- Publish information about appropriate use of social media relating to posts concerning the school.
- Seeking their permissions concerning digital images, cloud services etc
- Parents'/carers' evenings, newsletters, website, social media and information about national/local online safety campaigns and literature.

Parents and carers will be encouraged to support the school in::

- Reinforcing the online safety messages provided to learners in school.
- The safe and responsible use of their children's personal devices in the school (where this is allowed)

3. EXPECTED CONDUCT AND INCIDENT MANAGEMENT

3.1 EXPECTED CONDUCT

In this school, all users:

- Are responsible for using the school IT and communication systems in accordance with the relevant Acceptable Use Agreements;

- Understand the significance of misuse or access to inappropriate materials and are aware of the consequences;
- Understand it is essential to reporting abuse, misuse or access to inappropriate materials and know how to do so;
- Understand the importance of adopting good online safety practice when using digital technologies in and out of school;
- Know and understand school policies on the use of mobile and hand held devices including cameras;

3.2 STAFF, VOLUNTEERS AND CONTRACTORS

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

3.3 PARENTS/CARERS

- To support the school in students' use of the internet and other technologies.
- Should know and understand what the school's 'rules of appropriate use for the whole school community' are and what sanctions result from misuse.

3.4 INCIDENT MANAGEMENT

In this school:

- There is strict monitoring and application of the Online Safety policy and a differentiated and appropriate range of sanctions;
- All members of the school are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the school's escalation processes;
- Support is actively sought from other agencies as needed (i.e. the local authority, UK Safer Internet Centre helpline, CEOP, Prevent Officer, Police, Internet Watch Foundation) in dealing with online safety issues;
- Monitoring and reporting of online safety incidents takes place and contribute to developments in policy and practice in online safety within the school;
- Parents/carers are specifically informed of online safety incidents involving young people for whom they are responsible;
- The Police will be contacted if one of our staff or students receives online communication that we consider is particularly disturbing or breaks the law;
- We will immediately refer any suspected illegal material to the appropriate authorities – Police, Internet Watch Foundation and inform the LA.

4. MANAGING IT AND COMMUNICATION SYSTEM

4.1 INTERNET ACCESS, SECURITY (VIRUS PROTECTION) AND FILTERING

This school:

- Informs all users that Internet/e-mail use is monitored;
- Has the educational filtered secure broadband connectivity through the broadband provider
- uses a filtering system which blocks sites that fall into categories (e.g. adult content, race, ethnicity, religion or belief, sexual orientation, transgender identity, hate, gaming). All changes to the filtering policy are logged and only available to staff with the approved 'web filtering management' status;
- Ensures network health through use of anti-virus software

4.2 NETWORK MANAGEMENT (USER ACCESS, BACKUP)

This school:

- Uses individual, audited log-ins for all users – the network system;
- Uses guest accounts occasionally for external or short term visitors for temporary access to appropriate services;
- Uses teacher 'remote' management control tools for controlling workstations/viewing users/setting-up applications and Internet web sites, where useful;
- Ensures the Systems Administrator/network manager is up-to-date with local authority services
- Has daily back-up of school data (admin and curriculum);
- Storage of all data within the school will conform to the EU and UK data protection requirements; Storage of data online, will conform to the EU data protection directive where storage is hosted within the EU.

To ensure the network is used safely, this school:

- Ensures staff read and sign that they have understood the school's Online Safety policy. Following this, they are set-up with Internet, e-mail access and network access. This service is provided through a unique, audited username and password.
- All students have their own unique username and password which gives them access to the Internet and other services;
- Makes clear that no one should log on as another user and makes clear that students should never be allowed to log-on or use teacher and staff logins;
- Has set-up the network with a shared work area for students and one for staff. Staff and students are shown how to save work and access work from these areas;
- Requires all users to log off when they have finished working or are leaving the computer unattended;
- Ensures all equipment owned by the school and/or connected to the network has up to date virus protection;
- Makes clear that staff are responsible for ensuring that any computer or laptop loaned to them by the school, is used primarily to support their professional responsibilities.
- Makes clear that staff accessing LA systems do so in accordance with any Corporate policies;
  e.g. County e-mail or Intranet; finance system, Personnel system etc.
- Maintains equipment to ensure Health and Safety is followed;
- Ensures that access to the school's network resources from remote locations by staff is audited and restricted and access is only through school/LA approved systems:
- Does not allow any outside Agencies to access our network remotely except where there is a clear professional need and then access is audited restricted and is only through approved systems;
- This school uses secure data transfer; this includes DfE secure S2S website for all CTF files sent to other schools;
- Our wireless network has been secured to industry security level /appropriate standards suitable for educational use;
- All IT and communications systems installed professionally and regularly reviewed to ensure they meet health and safety standards;

4.3 PASSWORD POLICY

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

- We require staff to use STRONG passwords.
- We require staff using critical systems to use two factor authentication.

4.4 EMAIL

This school:

- Provides staff with an e-mail account for their professional use, LA/County hants.sch.uk e-mail and makes clear personal email should be through a separate account;
- We use anonymous or group email addresses, for example admissions@vyne.hants.sch.uk
- Will contact the Police if one of our staff or students receives an email that we consider is particularly disturbing or breaks the law.
- Will ensure that email accounts are maintained and up to date

Students:

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

Staff:

- Staff will use LA/County email system for professional purposes
- Access in school to external personal email accounts may be blocked
- The transfer of sensitive staff or student personal data via email should be protected with security encryption.

4.5 SCHOOL WEBSITE

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

4.6 LEARNING PLATFORMS

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

4.7 SOCIAL NETWORKING

Staff, Volunteers and Contractors

- Staff are instructed to always keep professional and private communication separate.
- Teaching staff are instructed not to run social network spaces for student use on a personal basis or to open up their own spaces to their students, but to use the schools' preferred system for such communications.
- Media for the use of any school approved social networking will adhere to school's procedures eg School Social Media Policy.

School staff will ensure that in private use:

- No reference should be made in social media to students, parents/carers or school staff;

- School staff should not be online friends with any student. Any exceptions must be approved by the Headteacher.
- They do not engage in online discussion on personal matters relating to members of the school community;
- Personal opinions should not be attributed to the school or Local Authority and personal opinions must not compromise the professional role of the staff member, nor bring the school into disrepute;
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Students:
- Are taught about social networking, acceptable behaviours and how to report misuse, intimidation or abuse through our online safety curriculum work.

Parents:
- Parents are reminded about social networking risks and protocols through the school website and additional communications materials when required.
- Are reminded that they need to ask permission before uploading photographs, videos or any other information about other people.

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

5. DATA SECURITY: MANAGEMENT INFORMATION SYSTEM ACCESS AND DATA TRANSFER

Strategic and operational practises

At this school:
- The Headteacher is the Senior Information Risk Officer (SIRO).
- We ensure staff know who to report any incidents where data protection may have been compromised.
- All staff are DBS checked and records are held in a single central record.

Technical Solutions
- Staff have a secure area(s) on the network to store sensitive files.
- We require staff to log-out of systems when leaving their computer, but also enforce lock-out after 30 minutes of idle time.
- All servers are in lockable locations and managed by DBS-checked staff.
- Details of all school-owned hardware will be recorded in a hardware inventory.
- Details of all school-owned software will be recorded in a software inventory.
- Disposal of any equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2006 and/or The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007. Further information can be found on the Environment Agency website.
- Where any protected or restricted data has been held we get a certificate of secure deletion for any server that once contained personal data.

6. EQUIPMENT AND DIGITAL CONTENT

6.1 PERSONAL MOBILE DEVICES (MOBILE PHONES, TABLETS AND OTHER MOBILE DEVICES) :

- Mobile devices brought into school are entirely at the staff member, students and parents or visitors' own risk. The school accepts no responsibility for the loss, theft or damage of any phone or handheld device brought into school.
- If students bring his or her mobile phone or personally-owned device into school and are seen using the device ***anytime*** (including break times) during the school day the device will be confiscated. Student personal mobile devices, which are brought into school, must be turned off (not placed on silent) and stored out of sight on arrival at school. They must remain turned off and out of sight until the end of the day.
- Personal mobile devices will not be used during lessons or formal school time unless as part of an approved and directed curriculum-based activity with consent from the classroom teacher.
- The Bluetooth or similar function of a mobile device should be switched off at all times and not be used to send images or files to other mobile devices.
- No images or videos should be taken on mobile devices without the prior consent of the person or people concerned.
- Staff members may use their phones during school break times not in front of students.
- The recording, taking and sharing of images, video and audio on any personal mobile device is to be avoided, except where it has been explicitly agreed by the Headteacher. Such authorised use is to be recorded. All mobile device use is to be open to monitoring scrutiny and the Headteacher is able to withdraw or restrict authorisation for use at any time, if it is deemed necessary.
- The School reserves the right to search the content of any mobile devices on the school premises where there is a reasonable suspicion that it may contain illegal or undesirable material, including pornography, violence or bullying. Staff mobile devices may be searched at any time as part of routine monitoring. Search processes are detailed in the Searching, Screening and Confiscation Policy.
- If a student needs to contact his or her parents or carers, they will be allowed to use a school phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office.
- Staff may use their mobile phones during break times. If a staff member is expecting a personal call they may leave their phone with the school office to answer on their behalf, or seek specific permissions to use their phone at other than their break times.

STORAGE, SYNCHING AND ACCESS

The device is accessed with a school owned account

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

The device is accessed with a personal account

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

STUDENTS' USE OF PERSONAL DEVICES

- The School strongly advises that student mobile phones and devices should not be brought into school.
- The School accepts that there may be particular circumstances in which a parent wishes their child to have a mobile phone for their own safety.
- If a student breaches the school policy, then the device will be confiscated and will be held in a secure place in the school office or the Family Support Team office. Mobile devices will be released to the student at the end of the school day or parents/carers in accordance with the school policy.
- Phones and devices must not be taken into examinations. Students found in possession of a mobile device during an exam will be reported to the appropriate examining body. This may result in the student's withdrawal from either that examination or all examinations.
- Students should protect their phone numbers by only giving them to trusted friends and family members. Students will be instructed in safe and appropriate use of mobile phones and personally-owned devices and will be made aware of boundaries and consequences.
- Students will be provided with school mobile devices to use in specific learning activities under the supervision of a member of staff. Such mobile devices will be set up so that only those features required for the activity will be enabled.

Staff use of personal devices

- Any permitted images or files taken in school must be downloaded from the device and deleted in school before the end of the day.
- Staff are not permitted (unless previously given permission by Headteacher/SLT) to use their own mobile phones or devices in a professional capacity, such as for contacting children, young people or their families within or outside of the setting.
- Staff will be issued with a school mobile phone where contact with students, parents or carers is required, for instance for off-site activities.
- Mobile Phones and personally-owned devices will be switched off or switched to 'silent' mode. Bluetooth communication should be 'hidden' or switched off and mobile phones or personally-owned devices will not be used during teaching periods unless permission has been granted by a member of the SLT in emergency circumstances.
- If members of staff have an educational reason to allow children to use mobile phones or a personally-owned device as part of an educational activity, then it will only take place when approved by the SLT/classroom teacher where appropriate.
- Staff should not use personally-owned devices, such as mobile phones or cameras, to take photos or videos of students and will only use work-provided equipment for this purpose.

- In an emergency where a staff member doesn't have access to a school-owned device, they should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes and then report the incident to a member of the SLT.
- If a member of staff breaches the school policy then disciplinary action may be taken.

6.2 DIGITAL IMAGES AND VIDEO

In this school:

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

NATIONAL LINKS AND RESOURCES

Action Fraud: www.actionfraud.police.uk
BBC WebWise: www.bbc.co.uk/webwise
CEOP (Child Exploitation and Online Protection Centre): www.ceop.police.uk
ChildLine: www.childline.org.uk
Childnet: www.childnet.com
Get Safe Online: www.getsafeonline.org
Internet Matters: www.internetmatters.org
Internet Watch Foundation (IWF): www.iwf.org.uk
Lucy Faithfull Foundation: www.lucyfaithfull.org
Know the Net: www.knowthenet.org.uk
Net Aware: www.net-aware.org.uk
NSPCC: www.nspcc.org.uk/onlinesafety
Parent Port: www.parentport.org.uk
Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline
The Marie Collins Foundation: http://www.mariecollinsfoundation.org.uk/
Think U Know: www.thinkuknow.co.uk
Virtual Global Taskforce: www.virtualglobaltaskforce.com
UK Safer Internet Centre: www.saferinternet.org.uk
360 Safe Self-Review tool for schools: https://360safe.org.uk/
Online Compass (Self review tool for other settings): http://www.onlinecompass.org.uk/

ANNEX 1

Computer Systems and Internet Agreement (Example)

Before students are allowed to use the computer systems and internet, we expect all students to read, sign and return this agreement. Students are responsible for good behaviour on the computer systems and internet just as they are in any other area of the school. The computer system is provided for students to conduct research and communications over the network. Individual users of the computer system are responsible for their behaviour and content of communications. Students are reminded that access is a privilege not a right and that access comes with responsibility.

It is presumed that ALL users will apply comply with school standards and honour this agreement that

1. The use of any school computer which provides access to the internet is a privilege which may be revoked by staff at any time for abusive or inappropriate conduct. Such conduct would include, but is not limited to, the placing of unlawful information on or through the computer system, accessing another person's files, account or email, and the use of obscure, abusive, or otherwise objectionable language or images in either public or private files or messages.
2. The school reserves the right to inspect any material stored in files to which users have access and will edit or remove any material which the staff, in its sole discretion, believes may be objectionable. Users of the computers and internet will not use their account to obtain, view, download or otherwise gain access to potentially objectionable materials. This includes text materials, video images or sound files that may be considered objectionable.
3. Information services and features contained on the school computer network are intended for the private use of the school. Any commercial or unauthorised use of those materials in any form is expressly forbidden.
4. The schools computers and network is intended for the exclusive use of its registered users. As a user, you are responsible for the use of your password and account. Any problems which arise from the use of a user's account are the responsibility of the account holder. Any misuse will result in suspension of the users account.
5. Deletion, examination, copying or modification of files and/or data belonging to other users without their prior consent is prohibited.
6. Any unauthorised, deliberate action which damages or disrupts a computing system (including the wilful introduction of computer "viruses" or other disruptive/destructive programs), alters its normal performance or causes it to malfunction is prohibited. Intended attempts to "crash" network systems or programs are punishable disciplinary offences.

Computer Systems and Internet Agreement

I have read the School Computer and Internet Usage Agreement, understand it, and agree to adhere to the principles and procedures listed within. I also understand that additional rules and regulations may be added from time to time and that they become a part of this agreement. Should I break this agreement, I understand that I may lose all computer and internet privileges. I also understand that inappropriate or illegal use of computer facilities could result in civil or criminal lawsuits. Parents and/or carers may be held accountable for inappropriate use by their child.

STUDENT AGREEMENT

As a school user of the computer systems and internet, I agree to comply with the above expectations.

Name .....

Signature of Student..... **Date**..... **Tutor**.....

We use photos and videos to promote our Students achievements throughout their time at The Vyne School. Sources of promotion are The School Website, Facebook, Twitter and our YouTube Channel. If you do not wish for them to have photos or videos taken, please let us know in writing or email admissions@vyne.hants.sch.uk

ANNEX 2

Acceptable User Policy (AUP)

1. Introduction

This ICT (Information and Communication Technology) Usage Policy outlines the guidelines and expectations for students' responsible and safe use of technology resources at Vyne. The purpose of this policy is to promote effective, secure, and ethical use of ICT tools and resources while fostering a positive learning environment for all students. All students must adhere to this policy while using any school-provided ICT resources, including computers, tablets, networks, internet access, and software applications.

2. Acceptable Use

2.1. Educational Purposes: ICT resources at Vyne are primarily for educational purposes. Students are encouraged to use technology to enhance their learning experiences, access educational resources, collaborate with peers, and complete school-related assignments and projects.

2.2. Respectful Communication: Students must communicate online with courtesy, respect, and appropriate language when interacting with teachers, peers, and other members of the school community. Bullying, harassment, or any form of offensive behaviour will not be tolerated.

2.3. Privacy and Data Protection: Students should respect the privacy of others and refrain from accessing, sharing, or distributing personal information without explicit permission. Any handling of sensitive data must comply with applicable data protection laws and school policies.

2.4. Copyright and Intellectual Property: Students must respect copyright laws and only use materials (text, images, videos, etc.) with proper permission or within the boundaries of fair use. Plagiarism and unauthorised distribution of copyrighted materials are strictly prohibited.

2.5. Security and System Integrity: Students must not attempt to access unauthorised areas of the school's ICT systems or disrupt the network's functionality. Any identified security vulnerabilities should be reported immediately to a teacher or school staff.

3. Internet Usage

3.1. Appropriate Websites: Students are only allowed to visit websites that are relevant to their educational activities. Inappropriate content, including but not limited to adult content, violence, gambling, or sites promoting illegal activities, is strictly prohibited.

3.2. Social Media and Online Communities: While the school recognizes the value of online communication, students must use social media and online platforms responsibly and during appropriate times, such as outside of instructional hours.

3.3. Cyberbullying and Online Safety: Students must not engage in cyberbullying or participate in any form of online harassment. Additionally, students should report any instances of cyberbullying to a teacher or school staff.

4. Device Usage

4.1. Responsible Device Use: Students should handle school-provided devices with care and use them for their intended educational purposes. Personalization and customization should not compromise the device's functionality or security.

4.2. Software Installation: Installing or downloading software on school devices without proper authorization is prohibited to maintain system integrity and security.

5. Consequences of Policy Violations

Any student found in violation of this ICT Usage Policy may face disciplinary action, which could include loss of ICT privileges, academic consequences, or other appropriate measures, as determined by school administration.

6. Policy Acknowledgment

By using Vyne's ICT resources, students acknowledge that they have read, understood, and agree to abide

by this ICT Usage Policy. Parents or guardians are encouraged to review this policy with their children to ensure compliance.

This ICT Usage Policy for students is subject to change as technology evolves and new challenges emerge. Regular reviews will be conducted to ensure its effectiveness in promoting a safe and conducive ICT environment for all students at Vyne school.

This document is automatically agreed to and signed when you sign the Home School Agreement