Online Safety and Use of Technology Policy

Document Title	Online Safety and Use of Technology Policy
Author	Head of ICLT
Version Number	Version 1.4
Approved by	Education and Safeguarding Committee
Effective from	October 2025
Due for Revision	October 2026

Prospect Trust Use of technology policy inside and outside of School/College

Table of Contents

Document Control Table

Document History			
Version	**Date**	**Author**	**Note of Revisions**
V1	Jan 2022	M Morren	First Trust-wide Use of Technology policy
V1.1	Oct 2023	M Morren	Updated name to include Online Safety 6. updated to National College 14.12 addition of guidelines from NC Cyber Security training 16.4 LGFL 360 safe 17.5 filters 'stress testing' 17.6 report to AQC governors 17.8 recognition of phishing, smishing and vishing 17.9 Cyber Security training AUP - change NOS to NC 17.10 added statement requested from Tomlinscote DSL
V1.2	May 2024	G Chapman	11.7 interim change - Members of staff are not permitted to make video or audio recordings of interactions with other staff members without their express permission. Learners, parents and carers are also forbidden from making video and audio recordings of interactions with staff without their express permission.
V1.3	June 2024	G Chapman	4.1 interim change – Suggestion from FCoEJS safeguarding audit – statement that online safety is part of computing curriculum. 9.2 interim change – Suggestion from TSS regarding the inclusion of the use of cellular/smart devices Appendix - Learner and Parent Use of Technology Policy - Learning
V1.4	Oct 2025	D Maguire	1.3 Addition of St Mark's 2.1 reference added to the Acceptable Use of Artificial Intelligence policy 4.2: reference to AI policy and education around the ethical use of AI in education 9.6 reference added to 2 Factor Authentication for access to Trust services (e.g. Google Workspace and Microsoft 365). 10.2: added reference to 2 Factor Authentication 17.11: Added reference to reporting content that is not filtered

1. Aims and scope

1.1. This policy has been written by The Prospect Trust, involving staff, learners and parents/carers, building on The Education People's mobile and smart technology policy template with specialist advice and input as required, taking into account the DfE statutory guidance 'Keeping Children Safe in Education', Early Years and Foundation Stage 'Working Together to Safeguard Children' and the local Surrey Safeguarding Children Partnership.

1.2. The purpose of this policy is to safeguard and promote the welfare of all members of The Prospect Trust community when using IT systems, mobile devices and smart technology. The Prospect Trust recognises that online safety is an essential part of safeguarding and acknowledges its duty to ensure that all learners and staff are protected from potential harm when using mobile and smart technology.

1.3. As outlined in our Child Protection Policy, the Designated Safeguarding Leads (DSL),

Matt Smith – The Sixth Form College Farnborough
Olivia Tolley – Tomlinscote School
Clare Wright/Sally Williams – Frimley Church of England Junior School
Rachel Jones/Jess Dustin - St Mark's C of E Primary School

are recognised as having overall responsibility for online safety.

1.4. This policy applies to all access to and use of all IT systems, mobile and internet connected devices on site; this includes mobile phones and personal devices such as tablets, e-readers, games consoles and wearable technology, such as smart watches and fitness trackers, which facilitate communication or have the capability to record sound or images.

1.5. This policy applies to learners, parents/carers and all staff, including the Academy Quality Councils, leadership team, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for, or provide services on behalf of the setting (collectively referred to as "staff" in this policy).

2. Links with other policies

2.1. This policy links with several other policies, practices and action plans, including but not limited to:

Anti-bullying policy
Acceptable Use Policies (AUP)
Acceptable use of Artificial Intelligence Policy
Behaviour Discipline Policy
CCTV Policy
Child protection and Safeguarding Policies
Code of conduct (values and ethos)
Data Protection Policy
Learning and Teaching Policy
Photographic images of Children Policy

Relationships and Sex Education Policy
Whistleblowing Policy

3. Safeguarding the welfare of children

3.1. The 'staying safe' outcome includes aims that children and young people are:

- Safe from maltreatment, neglect, violence and sexual exploitation
- Safe from accidental injury and death
- Safe from exposure to unacceptable content
- Safe from bullying and discrimination
- Safe from crime and anti-social behaviour in and out of School/College
- Secure, stable and cared for.

3.2. These aims apply equally to the 'virtual world' that children and young people will encounter whenever they use IT in its various forms. For example, there is a need to protect students from dangers such as:

- The use of the internet for grooming children and young people with the ultimate aim of sexual exploitation.
- The use of IT as a new weapon for bullies, who may torment their victims via websites, online forums, text or email messages.
- Exposure to inappropriate content when online, which can sometimes lead to their involvement in crime and anti-social behaviour.
- Inappropriate use of technology to create harmful content

3.3. It is the duty of all staff to ensure that every child in their care is safe, and the same principles should apply to the 'virtual' or digital world as would be applied to the School's/College's physical buildings.

4. Student education in the safe use of technology

4.1. All students will receive lesson time devoted to the safe use of technology. In the context of the College this is part of the tutorial programme, in the Schools, online safety is included as part of the statutory Computing curriculum and PSHE. Although it is vital that all teachers, when using technology / the internet, are cognizant of how to use these tools in a safe way, it is intended that this builds on the starting points all students gain in the PSHE / tutorial lessons.

4.2. Education around the safe use of technology also extends to the appropriate, and ethical, use of Artificial Intelligence to ensure that it is used as a tool for good. For more information, please refer to the Acceptable Use of Artificial Intelligence policy.

5. 'Safe Spaces'

5.1. The use of the term 'safe spaces' is encouraged to denote digital platforms in which it is safe to conduct communication, collaboration and data storage. These include, but are not limited to, Google Workspace, Microsoft Office, internal servers (e.g. CristalWeb at the College). Access to these services naturally varies with the age groups. All platforms used must have relevant checks and documentation (e.g. DPIAs) completed before they are permitted to be used.

5.2. For more information on how we access data please refer to our data protection policy

6. National College Platform

6.1. The academies throughout the Trust have access to the National College platform. This allows each Academy to share information and training resources to staff, parents and Academy Quality Councils. All resources shared can be logged and tracked.

Use of Devices

7. Trust Owned Digital Technology

7.1. Hardware, software and network resources purchased or provided by The Trust are to be used for creating, researching and processing Trust-related materials. All members of The Trust are responsible for exercising good judgement regarding the personal use of Trust resources. Storing personal files such as music, digital pictures and video on Trust systems is not permitted. Use of our cloud platforms (Apple iCloud, Google Workspaces, Office 365) for storing personal files is permissible but not recommended.

8. Trust Devices

8.1. By using the Trust's hardware, software and network systems, learners/staff assume personal responsibility for their appropriate use and agree to comply with this policy, as well as applicable laws and regulations. For learners below Year 7, this responsibility is shared by the supervising member of staff.

8.2. Trust devices and internet access are predominantly for the use of learning and teaching. Limited personal use of e-mail and internet is acceptable, but this must not interfere with the staff or students' work. Unreasonable personal use may amount to misuse of the facilities.

8.3. Devices and associated equipment must not be tampered with in any way.

8.4. Learners should not be using classroom equipment for personal study or use without prior permission of the member of staff and in their presence except in designated areas.

8.5. Executable files or files of any type that could cause damage to the Trust IT Systems may not be downloaded on to the network.

8.6. Where possible USB storage devices should not be used. However, if required, it is the user's responsibility that prior to being connected to the Trust IT System, they have been scanned for viruses/malicious files. The IT Support Department(s) can provide assistance if required.

8.7. The Trust has a number of designated shared use devices e.g. iPads, ChromeBooks and Laptops. These are for on-site use only; they should not be taken off site without direct permission from the relevant member of the IT Support Department(s) in each Academy.

8.8. All Trust devices are managed and therefore must be configured using the appropriate managed Trust account. E.g. Trust iPad – Managed Apple ID, Trust Chromebook – Managed Google Account.

8.9. All software must be deployed by the IT Support Department(s). Requests by learners/staff for software to be used on Trust devices are to be made to the IT Support Department(s) – software is not to be downloaded onto Trust devices without permission. The only exception will be in Computer Science and IT at the college where the use of 'local profile' installed software is common practice, this supports the specific courses.

8.10. Copyright or licensed software must be used in accordance with the relevant software license.

8.11. Any faults or damages to Trust devices must be reported to a member of the IT Support Department(s) as soon as possible.

9. Personal Devices - Safe Use

8.12. The Prospect Trust recognises that use of internet connected devices is part of everyday life for most people. Devices of any kind that are brought onto site are the responsibility of the user. All members of The Prospect Trust community are advised to:

- take steps to protect their mobile phones or personal devices from loss, theft or damage; we accept no responsibility for the loss, theft or damage of such items on our premises.
- use passwords/PIN numbers to ensure that unauthorised access, calls or actions cannot be made on their devices.

8.13. Mobile phones or smart devices with cellular connectivity are not permitted to be used on-site by any student below Year 12.

8.14. Learners and staff must not use devices in specific areas on site, such as changing rooms, toilets and swimming pools.

8.15. The sending of abusive or inappropriate messages or content via any device is forbidden by all members of The Prospect Trust community; any breaches will be dealt with in line with our anti-bullying, behaviour and child protection policies.

8.16. All members of The Prospect Trust community are advised to ensure that their mobile phones and personal devices do not contain any content which may be offensive, derogatory or illegal, or which would otherwise contravene our behaviour or child protection policies.

8.17. Staff must ensure that, when using a personal device to access Trust services, the device has appropriate antivirus software installed and running the latest security updates. Additionally personal devices should be secured with a password or passcode to prevent unauthorised access. 2 Factor Authentication should also be used to access Trust Services, e.g. Google Workspace and Microsoft 365.

9. Trust provided mobile phones

9.1. Some members of staff will be issued with a work phone number in addition to their work email address, where contact with learners or parents/carers is required.

9.2. Trust mobile phones and devices will be suitably protected via a passcode/password/PIN and must only be accessed or used by members of staff and/or learners. They should also use 2 Factor Authentication for further security.

9.3. Trust mobile phones and devices will always be used in accordance with the acceptable use of technology policy and other relevant policies.

9.4. Where staff and/or learners are using trust provided mobile phones and/or devices, they will be informed prior to use via this Use of Technology Policy that activity may be monitored for safeguarding reasons and to ensure policy compliance.

10. Staff use of devices

10.1. Members of staff will ensure that use of any devices, including personal phones and mobile devices, will take place in accordance with the law, as well as relevant Trust policy and procedures, such as confidentiality, child protection, data security staff code of conduct and use of technology policy.

Staff will be advised to:

- Keep mobile phones and personal devices in a safe and secure place during lesson time.
- Keep personal mobile phones and devices switched off or set to 'silent' mode during lesson times.
- Ensure that Bluetooth or other forms of communication, on a personal device, such as 'airdrop', are hidden or disabled during lesson times.
- Not use personal devices during teaching periods unless written permission has been given by the Principal or Headteacher in each Academy, such as in emergency circumstances. An exception to this would be to authorise Multi Factor Authentication prompts.
- Ensure that any content bought onto site via personal mobile phones and devices is compatible with their professional role and our behaviour expectations.

10.2. Members of staff are not permitted to use their own personal phones or devices for contacting learners or parents and carers.

- Any pre-existing relationships or circumstance, which could compromise staff's ability to comply with this, will be discussed with the DSL and/or Principal or Headteacher of each Academy.

10.3. Staff will only use Trust provided equipment (not personal devices):

- to take photos or videos of learners in line with our Photographic images of Children Policy
- to work directly with learners during lessons/educational activities. Staff may decide to use a personal device to communicate between themselves on an educational activity, i.e. a school trip/visit.
- to communicate with parents/carers.

10.4. Where remote learning activities take place, staff will use Trust provided equipment. If this is not available, staff will only use personal devices with prior approval from the Principal or Headteacher, following a formal risk assessment. Staff will follow clear guidance outlined in this Use of Technology policy and/or remote learning guidance.

10.5. If a member of staff breaches our policy, action will be taken in line with our staff code of conduct policy.

10.6. If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device or have committed a criminal offence using a personal device or mobile phone, the police will be contacted and the Local Authority Designated Officer (LADO) will be informed in line with our allegations policy.

10.7. Members of staff are not permitted to make video or audio recordings of interactions with other staff members without their express permission. Learners, parents and carers are also forbidden from making video and audio recordings of interactions with staff without their express permission.

11. Learner and Parent Use of Technology

11.1. Students must adhere to the Learner and Parent Use of Technology Agreement. This has been designed to keep them safe and happy online at home and at School/College. This is set out in Appendix 1.

12. Visitor Use of Technology

12.1. Parents/carers and visitors, including volunteers and contractors, are expected to ensure that:

- Mobile phones and personal devices are only permitted within specific areas and for specific purposes in each of the academies. E.g. for a multi-agency meeting
- Mobile phones and personal devices must not be used to take photos or video of any member of staff or learner, unless explicit consent has been given.
- Mobile phones and personal devices must not be used to record conversations with staff and/or learners, unless explicit consent has been given.

12.2. Appropriate signage and information is in place to inform visitors of our expectations for safe and appropriate use of technology.

12.3. Visitors, including volunteers and contractors, who are on site for regular or extended periods of time are expected to use technology in accordance with our Use of Technology Policy and other associated policies, including Child Protection.

12.4. If visitors require access to Trust Devices, for example when working with learners as part of multi-agency activity, this will be discussed with the relevant member of staff and the IT Support Department(s) prior to access being permitted.

- Any arrangements regarding agreed visitor access to technology will be documented and recorded by the Trust. This may include undertaking appropriate risk assessments if necessary.

12.5. Members of staff are expected to challenge visitors if they have concerns about their use of technology and will inform the DSL or Principal/Headteacher of any breaches of our policy.

13. Security and Passwords
Profiles and Accounts

13.1. Staff and pupils from Year 3 upwards are provided with ownership of a unique username and password combination. They are given access to a personal documents area and relevant shared areas. All account security events are logged.

13.2. In addition we also provide the opportunity to access our online educational domains as well as our internal School/College network. The Prospect Trust uses multiple educational providers, including Apple, Google and Microsoft, to provide a wide variety of learning tools, opportunities and benefits.

13.3. Apple 'iCloud', Google 'Workspace for Education' and Microsoft 'Office 365' are diverse collections of online tools for storage, collaboration, document creation and editing which can be accessed from any device. They are also used to synchronise information between School/College and personal devices, and

sign into additional education resources without a surplus of additional usernames and passwords.

13.4. Users must remember their association with and responsibility to The Prospect Trust in online social environments. If you identify yourself online as a member of the Prospect Trust Community, ensure your profile and related content is consistent with how you wish to represent yourself in person and will not bring the trust into disrepute.

13.5. Care should be taken when using last names, School/College names, addresses or phone numbers that appear online. Users should, when uploading digital pictures or avatars that represent themselves, be sure to select an appropriate image. They should also remember not to use copyrighted images.

13.6. All users of digital technology in the Prospect Trust have an obligation to ensure that any confidential Trust information is safeguarded. Any mobile devices that are configured with a Trust account should be secured with a minimum 6 digit passcode and/or biometric authentication which should never be disclosed to others under any circumstances.

Prospect Trust Network Passwords and Summary

13.7. All members of The Prospect Trust are regularly advised and reminded of the need to manage their password by training from IT teachers, automatically generated e-mails and direct communication from the IT Support Department(s).

13.8. The below table summarises the password policy enforcement for staff, students and guest accounts. This strategy is in support of SSO (single sign on) to online providers used by the School/College such as Office 365 and G Suite for Education. In all cases, staff and students are required to respect password privacy and model good practice.

User Account	Password Criteria	Details
Staff	8+ characters Complex password No expiration MFA Enforced	This includes all teaching & support staff including Governors, supply/assistant teachers, IT support, staff helpers and auditors/inspectors. MFA enforced for all external access, and Remote Access
KS5 Students	8+ characters Complex password No expiration MFA Enforced	Students conform to the same high standards of password complexity and independence as staff. MFA enforced for all external access, and Remote Access?
KS3/KS4 Students	8+ characters Complex password No expiration	Students conform to the same high standards of password complexity and independence as staff.
KS2 Students	8+ characters Optional complexity No expiration	Students in KS2 can begin to use an enhanced alphanumeric password, with guidance from staff.
Shared or Guest Accounts	8+ characters Complex password No expiration	Low risk accounts used for guest, presentation, exam, or network purposes. Typically, low access or short-term accounts such as Visitors and Events.

13.9. Passwords are stored with non-reversible encryption by The Prospect Trust and are not retrievable or accessible by the IT Support Department(s). The user account and content within remains the property of The Prospect Trust, and if intervention or help is required, the password will be reset.

13.10. All users are responsible for the safekeeping of their School/College credentials. Access to the system must only be made with the user's own account and password, which must not be given to any other person except where expressly permitted by the IT System Managers of each Academy.

Complex Password Guidelines

13.11. The popular definition of a complex password and the requirements are:

- Must be unique
- May not contain any 3 consecutive characters from your names or your username
- A minimum of eight characters, and containing characters from at least three of the following groups:
    - Uppercase letters - A, B, C ...
    - Lowercase letters - a, b, c ...
    - Numerals - 0,1,2,3,4,5,6,7,8,9
    - Symbols - ` ~ ! @ # $ % ^ & * ( ) _ + - = { } | \ : " ; ' < > ? , . /
- Complex passwords are automatically rejected if they do not meet these criteria.

Creating a Strong Password

13.12. A strong password is one that is easy for you to remember but difficult to crack by automated guesswork or discern from a previous version of the password. To make your password more secure, some suggestions are:

- Compact a memorable sentence into a word. For example, "I have a rabbit called Dennis who eats Carrots." becomes "IharcDweC."
- Use three random unrelated words.
- Add a memorable date or string of numbers to your favourite word. You should not use your birthday, PIN or telephone number in any password
- Start or finish with a capital letter or punctuation symbol.
- Invent and follow a convention to cater for regular password changes. Note that this must ensure a more significant change with each version than merely incrementing numbers.

13.13. Avoid things which may cause your password to become weak or problematic:

- **Avoid complete standalone dictionary words.** For example, *Password* is a weak password. Additionally, don't use song lyrics, quotes or anything else that's been published. Attackers have massive databases of published works to build possible passwords from.
- **Don't place the words in a predictable pattern** or form a proper sentence; that would make it much easier to guess.
- **Don't use any personal information**. Even when combined with letters and numbers, someone who knows you, or can research you online, can easily guess a password with this information.

- **Avoid unusual symbols** such as # or @ or " which may not appear reliably on all keyboards.
- **Don't use the same password twice.** Many popular websites fail to adequately secure your password in their systems, and hackers routinely break into them and access hundreds of millions of accounts. If you reuse passwords from site to site, then someone who hacks into one site will be able to login to your account on other sites. At the very least, make sure that you have unique passwords for all sites that store financial or other sensitive data, or ones that could be used to hurt your reputation.
- **Don't share your passwords.** Even if you trust the person, it's possible an attacker could intercept or eavesdrop on the transmission, or hack that person's computer. If you suspect that someone else knows your password, you should change it immediately.
- **Do not write down your password**, but you may use approved methods to record passwords as part of a secure solution. See below or if in doubt, contact the IT Support Department(s).

13.14. Passwords of staff and students from Year 3 – 13 will be synchronised to their online Google and Microsoft accounts, and adhere to the password requirements set above. When a password is changed, please be aware that that password will also need updating on all devices for those online services.

Online Passwords Guidelines

13.15. Passwords for websites and online accounts are numerous and vary greatly in levels of risk and consequence. An ongoing strategy is advisable according to the nature and quantity of passwords involved.

13.16. For websites which hold a functioning email account or significant personal data/tracking, such as Apple, Google, Microsoft, Facebook, Twitter, it is advisable to use a strong, complex password which is unique to that website.

13.17. For websites which hold data about you, such as your real name or address, commit a strong, complex password to memory, or adopt a password convention.

13.18. For common and inconsequential websites that hold no data about you (not even your name) and represent an insignificant risk if they were compromised or hijacked, you may nominate an expendable password. You can use this same password across similar expendable websites without raising your risk profile.

14. Strategies for Managing Passwords and Multi Factor Authentication

14.1. You may leave an unlabelled hint to your password (for example, the numerical component disguised as a phone number, or the complete version of a compacted sentence) in a private location. This can serve as a discrete reminder but should not make your password obvious to anyone.

14.2. Formulating a convention for website passwords should be a personal invention. One example is to take the first and last letter of the website and add a memorable sequence of numbers and letters in between. This will not make other passwords obvious if a single website is compromised and your credentials are stolen.

14.3. Only the use of password management repositories, tools and software which have been approved by the IT Support Department(s), are permitted. Password

management software involves a master password, which must have the same or better security and exclusivity, than any of the passwords being protected.

14.4. The password management of modern browsers such as Safari, Google Chrome and Microsoft Edge allow passwords to be saved and auto-filled with greater convenience across all devices. On non-managed devices, the browser must be signed in with a Trust account before saving Trust passwords.

14.5. Multi Factor Authentication (MFA) or 2-Factor Authentication (2FA) is a gold standard of security, that is enforced for all staff and KS5 students across The Prospect Trust. Where possible, this should be enabled on any online accounts.

Internet Use & Online Safety

15. Internet Access

15.1. Internet access for all purposes is reviewed regularly by the IT Support Department(s) in each Academy. The Trust may exercise its right to monitor the use of its computer systems, including the monitoring of web-sites, the interception of e-mails and the deletion of inappropriate materials where it believes the Trust's computer system is being used inappropriately. All users have prescribed internet permissions that apply whilst accessing the Internet through any device.

15.2. In line with our aim to keep children safe from radicalisation and exposure to terrorist and extremist or potentially distressing material, The Trust additionally monitors and reports on related online activity. The level of monitoring and filtering is under constant review.

15.3. Access to the Internet is filtered and monitored by each Academy. Each site has both primary and backup internet connectivity, and no access to unfiltered internet is available. Unknown websites are blocked by default but can be requested via the relevant IT Support Department. The Safeguarding teams at each Academy are responsible for the monitoring.

15.4. Each academy has completed the LGFL 360 Safe audit tool and will continue to update the information as and when necessary, at least annually.

16. Internet Filtering and Monitoring

16.1. Each Academy provides user-based internet filtering, allowing an appropriate level of browsing permission for the relevant age group, following the guidance from the DfE's KCSIE document.

16.2. The following are examples of blocked categories: Proxy Avoidance, Gambling, Nudity, Spam, Drugs, Dating, Illegal, Radicalisation, Weapons, Hate, Racism, Violence.

16.3. Websites and services are reviewed individually from permitted categories such as social media, entertainment, streaming media and instant messaging. Disreputable or compulsive services such as Snapchat and Netflix are carefully reviewed, and additional controls may be imposed at any time.

16.4. All users of the Trust networks must adhere to internet controls in place and no attempts to bypass them are permitted. Services such as VPNs (Virtual Private Networks) and Proxy Servers are blocked whilst connected to a Trust network. For their own safeguarding, their devices must be within the protection of the Trust's controls.

16.5. Filters are regularly 'stress tested' by the academy DSL's to ensure that they continue to provide a robust service and keep Prospect Trust staff and students

safe. If a weakness is found it will be reported to the IT Support Departments immediately.

16.6. Filter logs and testing documents are shared with AQC governors each half term. All unique devices attached to the network will be included in this report eg iPads, Chromebooks, PC's & Laptops. All types of accounts will also be checked: students, staff and visitors.

16.7. In the event of accidental breach, please seek the immediate guidance and support of the IT Support Department(s).

16.8. All staff to understand that there may be attempts to compromise the network via Phishing, Smishing & Vishing and can recognise these and report these attempts to IT Support.

16.9. All staff will complete a Cyber Security course at least annually either NCSC or NC.

16.10. All staff are responsible for promoting and supporting safe behaviours in their classrooms and for following Online-Safety procedures.

16.11. Staff should report any inappropriate content that is not filtered to the IT Support Team immediately.

17. Mobile Data

17.1. When staff are provided with 3G/4G enabled devices – in particular phones - the trust cannot guarantee protection from inappropriate websites. The ultimate protection is in the good sense of staff knowing what is available to them and the risks to which they may be subject.

18. Social Media Guidelines

18.1. The term "social media" encompasses social networking sites such as, but not limited to, Facebook, Instagram, WhatsApp, Snapchat and Twitter, as well as to more general types of social media and instant messaging such as, but not limited to, blogs, wikis, podcasts and digital images/videos.

18.2. The lines between public and private, personal and professional can easily become blurred in the digital world.

- All members of The Trust are personally responsible for the content they publish online. Users should be mindful that what they publish will be published for a long time. Future employers could access even your earliest posts on social media. Publishing any material that defames the Trust will always be dealt with as a serious disciplinary matter.
- Online behaviour should reflect the same standards of honesty, respect, and consideration that is expected when conversing face-to-face. What is inappropriate in the classroom should be deemed inappropriate online.
- When contributing online, do not post confidential or personal information.
- Comments made on sites such as Twitter are not protected by privacy settings. The Prospect Trust Community should be aware of the public and widespread nature of such media.
- By posting comments, having online conversations, etc. you are broadcasting to the world. Be aware that even with the strictest privacy settings what is 'said' online should be within the bounds of discretion. Comments expressed via social networking pages under the impression of a 'private conversation' may still end up being shared in a more public domain, even with privacy settings on maximum.
- Teachers and other staff members must not add students as 'friends' on social networking sites, i.e. visibility of either party's private profiles should not be allowed. The exception to this rule is immediate family members. This is for the

protection of both students and staff; failure to follow this guidance could result in disciplinary action.

- Before posting photographs and videos, permission should be sought or already sought as part of a learner's agreement, from the subject where possible. Staff posting photographs of students on the Academy websites for news or PR purposes should check that they do not feature any student for whom permission has not been granted by their parents/guardians for photographs to be used. No photograph of a students on the public section of the website will feature a student's full name.
- Before posting personal photographs, thought should be given as to whether the images are appropriate. Personal connections on social media between current or recently departed students and staff social media accounts are not allowed.

19. Trust Email System

19.1. The Trust provides an email system that is accessible to all members. They must use this to communicate with each other and make no use of personal email addresses for School/College business. Safeguarding regulations preclude staff from contacting students by any other address.

19.2. Email accounts may be set up on personal devices to enable receipt of School/College emails whilst on or off Trust premises if desired. It is best practice to use official email clients where possible e.g. Google Mail, Outlook.

19.3. Emails from suspicious sources should not be opened. These should be reported to the IT Support Department(s).

19.4. Staff should not direct students or families to make use of private communication mechanisms as part of lesson delivery and private study. For example, requesting students use chat rooms and private forums, outside of official Trust platforms, is not permissible.

19.5. Staff should always bear in mind when communicating by email that in law, an email is a document which may be disclosable in legal proceedings and in the event of a subject access request. All email messages sent or received within the Trust email system are the property of the Trust and users should not expect personal privacy when using the email system. The IT Systems Manager is authorised to monitor email messages and network logs and to nominate members of the IT Support Department(s) to do the same so as to ensure compliance with Trust policies. All users agree to such monitoring and reviewing of emails.

19.6. The content of all emails must not contain offence or harassment of a sexual, racial or religious nature, whether explicit or implicit, and must be written using only vocabulary acceptable for professional communication in the workplace.

19.7. Confidentiality is not guaranteed. Any message sent or received may be accessed by colleagues other than the individual to whom it is sent, whether by accident (e.g. a computer left logged on) or design (e.g. an email may need to be opened to diagnose connectivity problems). Messages cannot therefore be regarded as private or confidential. Personal messages should be written remembering this possibility for third parties to review the content. In the case of external email, there is no inherent security at all and such messages can potentially be intercepted and read by third parties without our knowledge. Messages of particular confidentiality or sensitivity should be sent by an alternative medium.

19.8. Users should not use the Trust's email for participation in chain letters, soliciting for charitable endeavours, either their own or on behalf of others, or distributing material which violates or infringes the intellectual property rights (including

copyright, patent or trademarks rights) of any other person or organisation (including the Trust).

19.9. Any email sent out using Trust email systems will be sent from the Trust and may therefore impact upon the reputation of the Trust. In the same way, accessing the Internet from a Trust network means that it is the Trust accessing the site, not just the user in a personal capacity.

20. Remote Access

20.1. The Prospect Trust staff have the facility to access the trust network resources whilst away from School/College via our Remote Desktop facility. Staff and students are required to be vigilant when accessing systems remotely. Computers or other digital devices should not be left unattended when connected.

- Remote users will be disconnected if left unattended for an extended period of time.
- Remote users need to pass additional security checks i.e. re-entry of their School/College password
- Remote users must make sure they are not being overlooked by anyone, even family, when accessing confidential data.
- Network access should not be shared with friends or family members, and they should not use the Trust system.

21. Responding to Policy Breaches

21.1. All members of the community are informed of the need to report policy breaches or concerns in line with existing Trust policies and procedures. A list is at the beginning of this document.

21.2. After any investigations are completed, leadership staff will debrief, identify lessons learnt and implement any policy or curriculum changes, as required.

21.3. We require staff, parents/carers and learners to work in partnership with us to resolve issues.

21.4. All members of The Prospect Trust community will respect confidentiality and the need to follow the official procedures for reporting concerns.

21.5. Learners, parents/carers and staff will be informed of our complaints procedure and staff will be made aware of the whistleblowing policy.

21.6. If we are unsure how to proceed with an incident or concern, the DSL (or a deputy) or Principal/Headteacher will seek advice from the Surrey Safeguarding Children Partnership or Hampshire Safeguarding Children Partnership other agency in accordance with our child protection policy.

22. Policy monitoring and review

22.1. Technology evolves and changes rapidly. The Prospect Trust will review this policy at least annually. The policy will be revised following any national or local policy updates, any local concerns and/or any changes to our technical infrastructure.

22.2. We will regularly monitor internet use taking place via our provided devices and systems and evaluate online safety mechanisms to ensure that this policy is consistently applied. Any issues identified will be incorporated into our action planning.

22.3. All members of the community will be made aware of how the Trust will monitor policy compliance.

I understand my responsibilities as described in this Use of Technology Policy:

Signed:

Print Name:

Date:

Appendices

Learner and Parent Use of Technology Policy

I understand that Learner and Parent Use of Technology Agreement will help keep me safe and happy online at home and at School/College.

Learning

- I know that Prospect Trust computers, devices and internet access have been given to me to help me with my learning
- I know that other types of technology may not be allowed. If I am not sure if something is allowed, I will ask a member of staff.
- If I need to learn online at home, I will follow the Prospect Trust remote learning guidance.
    - Frimley CofE Junior School
    - Tomlinscote School
    - Farnborough 6th Form College
    - St Mark's Church of England Primary School
- I will only use my iPad or PC in School/College if I have permission from a teacher.
- Mobile phones or any other devices that can be used to make or receive calls are not permitted at Frimley Junior, St Mark's and Tomlinscote School. Year 5 and 6 children, who walk to and from school, are allowed to bring a mobile phone to school. When in school, all mobile phones must be handed in to the school office upon arrival and collected at the end of the day,

Safe

- I will make sure that my internet use is safe and legal, and I am aware that my actions online have offline consequences. For more information you can use the websites below:
    - https://saferinternet.org.uk
    - https://www.thinkuknow.co.uk
    - https://nationalonlinesafety.com
- I know that my use of School/College devices and internet access will be monitored, at home and at School/College, to protect me and to make sure I follow the acceptable use policy.
- I know that people online are not always who they say they are and that I must always talk to an adult before meeting any online contacts.

Private

- I will not share my passwords with anyone.
- I will check my privacy settings with an adult to make sure they are safe and private.
- I will think before I share personal information and always seek advice from an adult if I'm unsure.
- I will keep my password safe and private as my privacy, School/College work and safety must be protected.

Responsible

- I will not use or access other learners' devices
- I will not access or change other people's files, accounts, or information unless I have been asked to collaborate on a piece of work.
- I will only upload appropriate pictures or videos of others online when I have their permission.
- I know I must respect the School/College internet access and equipment and if I cannot be responsible then I will lose the right to use them.
- I will write emails and online messages carefully and politely as I know they could be forwarded or seen by someone I did not expect.
- I will only change the settings on the computer if a teacher/technician has allowed me to.
- I know that use of the Prospect Trust ICT systems for making money, gambling, political purposes is not allowed. I am not allowed to advertise anything.
- I understand that the School/College internet filter is there to protect me, and I will not try to bypass it.
- I know that if the trust suspect that I am behaving inappropriately with technology, then my use will be investigated. My devices, such as iPad/ChromeBook may be checked and/or taken away from me.
- I know that if I do not follow the Prospect Trust Acceptable Use Policy then the following sanctions/processes maybe used:
    - Interview, counselling and/or disciplinary action by tutor, Head of Year, Online Safety Coordinator, Child Protection Officers, Principal/Headteacher;
    - Informing parents or carers;
    - Removal of Internet or computer access for a period, [which could ultimately prevent access to files held on the system, including examination coursework];
    - Referral to the Local Authority / Police and/or other external agencies for safeguarding purposes.

Kind

- I know that bullying in any form (on and offline) is not allowed; technology should not be used for any form or abuse or harassment.
- I will not upload or add any images, video, sounds or text that could upset, threaten the safety of or offend any member of the School/College community.

- I will always think before I post as text, photos or videos can become public and impossible to delete.
- I will not use technology to be unkind to others.

Legal

- I know cybercrime can be a criminal offence, for example gaining unauthorised access to systems ('hacking') and making, supplying or obtaining malware.
- I know it can be a criminal offence to send threatening and offensive messages.
- I will respect other people's information and copyright by giving a reference and asking permission before using images or text from online sources.
- I understand that it may be a criminal offence or against the rules of the School/College policy to download or share inappropriate pictures, videos, or other material online.

Reliable

- I will always check that any information I use online is true and accurate.
- I know that people I meet online may not be who they say they are. If the adult deems it safe to meet this person, I will always meet in a public place with a trusted adult present.

Report

- If I know of anyone trying to misuse technology, I will report it to a member of staff.
- I will speak to an adult I trust if something happens to either myself or another learner which makes me feel worried, scared, or uncomfortable.
- I will visit www.thinkuknow.co.uk, www.childnet.com, www.childline.org.uk and https://nationalcollege.com to find out more about keeping safe online.
- I have read and talked about these expectations with my parents/carers.

Online Accounts

- The creation and use of a Trust Apple 'iCloud', Google 'Workspace for Education' and Microsoft 'Office 365' account, as per the Use of Technology Policy, incorporate the workflow which has been developed for the learners, along with ensuring that documents are backed up safely.
- By signing this agreement, you give permission for the Trust to create online Apple, Google and Microsoft accounts as part of this agreement, and other additional learning based accounts as required. For learners under the age of 13, permission is given on their behalf, by the parent signing this agreement. These organisations respect the data privacy of schools/colleges in their educational software products, and learner data is not used for commercial or advertising purposes, and remains the property of the School/College.

Learner and Parent IT Acceptable Use of Technology Agreement

Please complete and return a separate form for each learner.
I confirm that we have read the Use of Technology Policy. We accept the terms of the Learner and Parent IT Acceptable Use of Technology Agreement regarding the proper use of technology and agree to abide by them, including the creation of accounts.

Learner Name:	_____	Signature:	_____
Parent/Carer Name:	_____	Signature:	_____
Date:	_____		