Acceptable Use Policy & Procedure

Incorporating Email, Social Media & Blended Learning

Document control			
Document Suite:	**Human Resources**	**Document Title:**	Acceptable Use Policy & Procedure Incorporating Email, Social Media & Blended Learning
Document Type:	Policy (Internal)	**Version number:**	2
Author (name & job title):		Nina Adams Director of HR	
Date Formally approved:	***24th November 2021***	**Formal Approval by:**	***Trust Board PPP Committee***
Review information:	**Scheduled**	**Next Review Due By** 31st August 2026	

Document History			
Version	***Date***	***Reviewer***	***Note of revisions***
V1	01/03/2022	n/a	Implementation
V2	14/10/2024	N Adams	Updated guidance, updated values

1. **Scope**

1.1 This policy applies to all users of Pathfinder Schools Trust information and relates to the use of all IT facilities and services provided by Pathfinder Schools. This applies not only to the use of Trust digital technology equipment within the workplace but also to the use of Trust systems and equipment outside of Trust premises and the use of any personal devices or equipment on or off school premises.

2. Context

2.1 Pathfinder Schools understands that Information Communication Technology (ICT) is an integral and critical resource for students, staff, governors, volunteers, and visitors through the delivery and support of teaching and learning and supporting pastoral and administrative functions of the Trust and its academies. However, the Trust accepts that the ICT resources and facilities our academies use also pose risks to data protection, online safety, and safeguarding.

3. Purpose

3.1 The purpose of this policy is to ensure that employees, workers, visitors, and other people accessing Trust Information Communication Technology (ICT) understand how it may be used.

4. Policy aims

4.1 Pathfinder Schools' intended aim is to provide an ICT provision that promotes educational excellence and innovation, whilst educating users about online behaviour, including interacting with other individuals on social networking websites and in chat rooms and cyberbullying awareness.

4.2 This policy aims to:

- Safeguard and protect all members of the Pathfinder Schools Community
- Identify approaches to educate and raise awareness for online safety
- Enable all staff to work safely and responsibly, to role model positive behaviour online, and to manage professional standards and practice when using technology
- Identify clear procedures to use when responding to online safety concerns
- Set guidelines and rules around the use of Trust ICT resources for staff
- Establish clear expectations for the way members of the Pathfinder Schools community engage with each other online
- Support the Trust's policy on data protection, safeguarding & child protection.
- Prevent disruption to the Trust through the misuse, or attempted misuse, of ICT systems
- Support the Trust and its schools in teaching students safe and effective internet and IT use
- Promote safe working practices for staff and students for remote learning during the COVID-19 global pandemic and beyond

5. Expectations

5.1 The Trust provides information systems for the use of all staff, students, governors, volunteers, and visitors on the understanding that:

- The user has read and agreed to abide by this policy.
- The user does not misrepresent themselves or attempt to impersonate another person or entity while using Trust IT systems.

- The user does not publish libelous material using the Trust IT systems e.g. via blogs or online journals or videos published on social media.
- Pathfinder Schools reserves the right to suspend access, retain equipment loaned to staff or students, and view any data held on its systems whilst investigating a breach of this policy or whilst investigating any other matter in which Pathfinder Schools has a legitimate interest.

5.2 Users are responsible and personally accountable for their use and activity on the Trust's ICT systems and Wi-Fi. Any use that contravenes this policy may result in the Pathfinder Schools Disciplinary Policy being invoked. In addition, ICT usage privileges may be withdrawn or reduced.

5.3 The Trust and its academies have the right to monitor the use of all devices including mobile devices issued, for internet use, e-mails, and all aspects of the network/computer system.

5.4 Breaches of this policy may be dealt with under our disciplinary and code of conduct policy and procedures.

6. Review

6.1 This policy will be monitored as part of the Trust Policy review cycle and as and when required by statutory changes.

7. Personnel responsible for implementing the policy

7.1 The Pathfinder Schools CEO and Trust Board have overall responsibility for monitoring the effectiveness of this policy, ensuring that a consistent approach to ICT is applied across the Trust and that this document is compliant with relevant legislation.

7.2 The CEO is responsible for ensuring that Heads are aware of this policy and that they have implemented effective measures for training, monitoring, and where appropriate incident response and investigation.

7.3 Day-to-day responsibility for operating the policy has been delegated to Head Teachers supported by the Pathfinder Schools Director of IT. Heads should ensure that employees receive training and guidance on the policy and in safe ICT and social media use. Heads will take a lead role in investigating any reported incidents and taking any further action in response to the incident.

7.4 The Pathfinder Schools IT colleagues (school and centrally engaged) will limit access to websites and may be directed to monitor usage and report any breaches to the appropriate Headteacher or CEO if breaches relate to central team members.

7.5 Managers must ensure they report any breaches of this policy immediately to the Headteacher.

7.6 All users must ensure they understand and adhere to the Trust's expectations regarding electronic usage and communications, seeking further clarification and advice where appropriate. If they require access to a website, which is blocked, they should raise the issue with their line manager and the IT Department.

8. Related Pathfinder Schools Policies

This policy should be read alongside Pathfinder Schools policies on:

- Safeguarding and child protection
- Student/pupil behaviour policy
- Code of Conduct
- Disciplinary Policy
- Data Protection/GDPR

9. Relevant legislation and guidance

9.1 This policy refers to, and complies with, the following legislation and guidance:

- Data Protection Act 2018
- The UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020
- Computer Misuse Act 1990
- Human Rights Act 1998
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Education Act 2011
- Freedom of Information Act 2000
- Education and Inspections Act 2006
- Keeping Children Safe in Education 2023
- Searching, screening and confiscation: advice for schools 2022
- National Cyber Security Centre (NCSC): Cyber Security for Schools
- Education and Training (Welfare of Children) Act 2021
- UK Council for Internet Safety (et al.) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Meeting digital and technology standards in schools and colleges

9.2 All policies and guidelines referred to in Pathfinder Schools policies are available upon request from the School/Academy HR Representative.

10. Definitions

"ICT facilities": includes all facilities, systems, and services including but not limited to network infrastructure, desktop computers, laptops, tablets, phones, music players or hardware, software, websites, web applications or services, and any device system or service which may become available in the future which is provided as part of the ICT provision

"Users": adults authorised by Pathfinder Schools to use the ICT facilities, including governors, staff, volunteers, contractors, and visitors

"Personal use": any use or activity not directly related to the users' employment, or purpose.

"Authorised personnel": employees authorised by the school to perform systems administration and/or monitoring of the ICT facilities.

"Materials": files and data created using the ICT facilities including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites, and blogs

11. Parents

11.1 Access to ICT facilities and materials

Parents/carers do not have access to the Trust's ICT facilities as a matter of course.

However, parents/carers working for, or with, the school in an official capacity (for instance, as a volunteer or as a member of the PTA) may be granted an appropriate level of access, or be permitted to use the Trust;s facilities at the headteacher's discretion.

Where parents/carers are granted access in this way, they must abide by this policy as it applies to staff.

11.2 Communicating with or about the school online

We believe it is important to model for pupils, and help them learn, how to communicate respectfully with, and about, others online.

Parents/carers play a vital role in helping model this behaviour for their children, especially when communicating with the school through our website and social media channels.

We ask parents/carers to sign the agreement in appendix 2.

11.3 Communicating with parents/carers about pupil activity

The Trust will ensure that parents and carers are made aware of any online activity that their children are being asked to carry out.

When we ask pupils to use websites or engage in online activity, we will communicate the details of this to parents/carers in the same way that information about homework tasks is shared.

In particular, staff will let parents/carers know which (if any) person or people from the school pupils will be interacting with online, including the purpose of the interaction.

Parents/carers may seek any support and advice from the school to ensure a safe online environment is established for their child.

12. Pupils

12.1 Access to ICT facilities

The following ICT Facilities are available to pupils:

- Computers and equipment in the Trust ICT suites and classrooms are available to pupils only under the supervision of staff
- Pupils will be provided with a Microsoft 365 account which will give them access to Teams, SharePoint and OneDrive

12.2 Search and deletion

Under the Education Act 2011, the headteacher, and any member of staff authorised to do so by the headteacher, can search pupils and confiscate their mobile phones, computers or other devices that the authorised staff member has reasonable grounds for suspecting:

- Poses a risk to staff or pupils, **and/or**
- Is identified in the school rules as a banned item for which a search can be carried out **and/or**
- Is evidence in relation to an offence
- This includes, but is not limited to:
- Pornography
- Abusive messages, images or videos
- Indecent images of children
- Evidence of suspected criminal behaviour (such as threats of violence or assault)
- Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:
- Assess how urgent the search is and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from Headteacher or their designate
- Explain to the pupil why they are being searched, and how and where the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's co-operation, if the pupil refuses to co-operate, the Trust's behaviour policy will be followed the authorised staff member should:
- Inform the DSL (or deputy) of any searching incidents where they had reasonable grounds to suspect a pupil was in possession of a banned item.
- Involve the DSL (or deputy) without delay if they believe that a search has revealed a safeguarding risk

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on a device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on a device, the staff member should only do so if they reasonably suspect that the data has been, or could be, used to:

- Cause harm, **and/or**
- Undermine the safe environment of the school or disrupt teaching, **and/or**
- Commit an offence

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL and/or to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding whether there is a good reason to erase data or files from a device, staff members will consider whether the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the

device will be handed to the police as soon as is reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, **and/or**
- The pupil and/or the parent refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image
- **Not** copy, print, share, store or save the image
- Confiscate the device and report the incident to the DSL (or deputy) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on searching, screening and confiscation and the UK Council for Internet Safety (UKCIS) et al.'s guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS et al.'s guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Our behaviour policy and approach on searches and confiscation
- Any complaints about searching for, or deleting, inappropriate images or files on pupils' devices will be dealt with through the school complaints procedure.

6.3 Unacceptable use of ICT and the internet outside of school

The Trust will sanction pupils, in line with the Behaviour Policy if a pupil engages in any of the following **at any time** (even if they are not on school premises):

- Using ICT or the internet to breach intellectual property rights or copyright
- Using ICT or the internet to bully or harass someone else, or to promote unlawful discrimination
- Breaching the Trust's policies or procedures
- Any illegal conduct, or making statements which are deemed to be advocating illegal activity
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate
- Consensual or non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams (also known as sexting or youth produced sexual imagery)
- Activity which defames or disparages the school, or risks bringing the school into disrepute
- Sharing confidential information about the school, other pupils, or other members of the school community
- Gaining or attempting to gain access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel
- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the Trust's ICT facilities
- Causing intentional damage to the Trust's ICT facilities or materials

- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user and/or those they share it with are not supposed to have access, or without authorisation
- Using inappropriate or offensive language

8. **Unacceptable use**

8.1 The following are examples of actions that will be considered as unacceptable use of the Trust's ICT facilities.

- Using ICT facilities to breach intellectual property rights or copyright
- Using ICT facilities to bully or harass someone else, or to promote unlawful discrimination
- Breaching the Trust's policies or procedures
- Any illegal conduct, or statements that are deemed to be advocating illegal activity
- Accessing, creating, storing, linking to, or sending material that is pornographic, offensive, obscene, or otherwise inappropriate
- Activity which defames or disparages the Trust or risks bringing it into disrepute
- Sharing confidential information about the Trust, its schools, pupils, staff, or other members of the Trust community.
- Connecting any device to the Trusts ICT network without approval from authorised personnel
- Setting up any software, applications, or web services on the Pathfinder Schools network without approval by authorised personnel, or creating or using any program, tool, or item of software designed to interfere with the functioning of the ICT facilities, accounts, or data
- Gaining, or attempting to gain, access to restricted areas of the network, or any password-protected information, without approval from authorised personnel
- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the Trusts ICT facilities
- Causing intentional damage to ICT facilities
- Online gambling, inappropriate advertising, phishing and/or financial scams
- Removing, deleting, or disposing of ICT equipment, systems, programs, or information without permission by authorised personnel
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation
- Using inappropriate or offensive language
- Promoting a private business, unless that business is directly related to the school and promotion has been agreed by authorised personnel
- Using websites or mechanisms to bypass the Trust's filtering mechanisms
- Engaging in content or conduct that is radicalised, extremist, racist, antisemitic or discriminatory in any other way
- Using AI tools and generative chatbots (such as ChatGPT and Google Board):

- During assessments, including internal and external assessments, and coursework
- To write their homework or class assignments, where AI-generated text or imagery is presented as their own work

8.2 This is not an exhaustive list. Pathfinder Schools reserves the right to amend this list at any time. The Headteacher or any other relevant member of staff will use professional judgement to determine whether any act or behaviour not on the list above is considered an unacceptable use of the Trust's ICT facilities.

9. Exceptions from unacceptable use

9.1 Where the use of school ICT facilities (on the school premises and/or remotely) is required for a purpose that would otherwise be considered an unacceptable use, exemptions to the policy may be granted at the headteacher's discretion.

9.2 Further to permission from the Headteacher or their designate Pupils may use AI tools and generative chatbots:

- As a research tool to help them find out about new topics and ideas
- When specifically studying and discussing AI in schoolwork, for example in IT lessons or art homework about AI-generated images. All AI-generated content must be properly attributed

14.3 Sanctions

14.5 Pupils and staff who engage in any of the unacceptable activities listed above may face disciplinary action in line with the Trust's policies on pupil behaviour and the staff Code of Conduct and Disciplinary Policy.

15. In the event of staff misuse

15.1 If an employee is believed to have misused the internet or school network in an illegal, inappropriate or abusive manner, a report must be made to the Headteacher/DSL immediately. Advice may be sought from the Trust HR Manager and IT Manager as appropriate15.2 The appropriate procedures for allegations must be followed and the following teams/authorities contacted where appropriate:

- Designated Officer (Previously LADO)

15.2 In the event of minor or accidental misuse, internal investigations should be initiated and staff disciplinary procedures followed only if appropriate.

16. Access to ICT facilities and materials

16.1 The Trust's ICT team manages access to the Trust ICT facilities and materials for staff. That includes, but is not limited to:

- Computers, tablets, and other devices
- Access permissions for programmes or files

16.2 Staff will be provided with unique log-in/account information and passwords that they must use when accessing the Trust's ICT facilities. Passwords should be kept secure, and where they are set by staff members should be strong.

16.3 Users are responsible for the security of their passwords and accounts, and for setting permissions for accounts and files they control.

16.4 Individuals who disclose account or password information may face disciplinary action and may have their access rights revoked.

16.5 All users of the Trust's ICT facilities will have clearly defined access rights to systems, files, and devices. These access rights are managed by the Pathfinder Schools IT Manager and are authorised by the Headteacher and the CEO where appropriate.

16.6 Gaining or any attempts to gain, access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel will be considered unacceptable use and a breach of this policy.

16.7 If access is provided in error, or if something a user should not have access to is shared with them, they should alert their line manager immediately.

16.8 Users should always log out of systems and lock their equipment when they are not in use to avoid any unauthorised access. Equipment and systems should always be logged out of and closed down completely at the end of each working day.

16.9 The only software authorised for use on Pathfinder Schools information systems are those programs already installed on the machinery by the ICT team or authorised for use in Trust activities. This includes online services.

16.10 Any attempt to introduce or install software onto the Academy or Trust systems will be viewed as an intention to damage Pathfinder Schools property and could constitute a breach of safeguarding and/or data protection regulations, resulting in disciplinary action.

16.11 Any user who causes damage, directly or indirectly, to any equipment may be refused the right to further use of the equipment and billed for its repair or replacement.

17. Remote access

17.1 We allow staff to access the Trust's ICT facilities and materials remotely. Including a small number of staff who access systems via a virtual private network (VPN).

17.2 The Trust IT Team manage remote access, security arrangements, and protocols for remote access.

17.3 Staff accessing the school's ICT facilities and materials remotely must abide by the same rules as those accessing the facilities and materials on site.

17.4 Staff must be particularly vigilant if they use the Trust's facilities outside the school and must take such precautions as the Director of IT and the IT Team may require against importing viruses or compromising system security.

17.5 Our ICT Facilities contain information which is confidential and/or subject to data protection legislation. Such information must be treated with extreme care and in accordance with our data protection policy.

18. Email communication at Pathfinder Schools

18.1The use of email at Pathfinder Schools is an essential means of communication for both adults and students. Educationally, email offers significant benefits including

direct written contact between schools on different projects, be they staff-based or student-based, within the school or in a wider context.

18.2In the context of the Trust, emails should not be considered private and staff should assume that anything they write or email could become public. Therefore, they should ensure that they are professional, maintaining a clear distinction between their personal and professional lives.

18.3Staff must take care with the content of all email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality, or breach of contract.

18.4Email messages are required to be disclosed in legal proceedings or in response to requests from individuals under the Data Protection Act 2018 in the same way as paper documents. Deletion from a user's inbox does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable.

18.5Any data exchanged with any external agency must be carefully reviewed to ensure compliance with the Trust's Data Protection Policy, particularly concerning the sharing of personal or sensitive data.

18.6The Trust provides adults with their own email account as a work-based tool. This account should be the account that is used for all Trust business. This is to minimise the risk of receiving unsolicited or malicious emails and avoid the risk of personal contact information being revealed.

18.7For the safety and security of users and recipients, all email is filtered and logged. If necessary, email histories can be traced.

18.8The following rules will apply:

- Under no circumstances should adults contact students, parents or conduct any school business using any personal email addresses.
- It is the responsibility of each account holder to keep their password/s secure.
- All external emails, including those to parents, should be constructed in the same way as a formal letter written on school headed paper
- If there are any concerns about the recipient i.e. complaints/issues, users are advised to cc their line manager/s and other relevant individuals into the email.
- The Trust requires a standard disclaimer to be attached to all email correspondence, clarifying that any views expressed are not necessarily those of the Trust. Please note that this disclaimer is automatically added to emails sent externally
- All emails should be written and checked carefully before sending.
- Emails created or received will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000.

18.9Adults are advised to manage their email account effectively as follows:

- Delete all emails of short-term value.

- Organise email into folders and carry out frequent housekeeping on all folders and archives.
- Respond to emails in a timely fashion, it is courteous to respond to emails within 24 hours.
- Staff must immediately inform the IT Manager if they receive an offensive email.
- Any suspicious emails are to be reported to the IT Manager and should not be opened

9.3 **Sending emails**

9.3.1 The following rules apply:

- When composing your message to a parent or non-staff member you should always use formal language as if you were writing a letter on headed paper.
- If an adult becomes aware they have sent an email in error that contains the personal information of another person, they must inform their Data Protection Lead immediately and follow the data breach procedure.

9.4 **Receiving emails**

The following expectations apply:

- If an adult receives an email in error, the sender should be informed and the email deleted. If the email contains sensitive or confidential information, the user must not make use of that information or disclose that information.
- Check your email regularly
- If appropriate, activate your 'out-of-office' notification when away for extended periods.
- Never open attachments from an untrusted source. If unsure, always consult the IT Manager first.
- Do not use email systems to store attachments. Detach and save Trust-related work to the appropriate shared drive/folder.
- The use of the Outlook setting to automatically forward and/or delete emails is prohibited at Pathfinder Schools.
- Individuals are required to 'manage' their accounts.

9.5 **Emailing personal, sensitive, confidential, or classified information**

- Assess whether the information can be transmitted by other secure means before using email
- Emailing confidential data without the use of encryption is strictly prohibited. Staff are required to read and understand the General Data Protection Regulation Policy and the expectations within it.
- Where the conclusion has been reached that a Trust email should be used to transmit such data, then the following steps should be followed;

I. Verify the details, including the accuracy of any email address used

II. Verify (preferably by phoning) the details of a requestor, if unknown, before responding to email requests for information.

III. Do not copy or forward the email to any more recipients than is necessary.

IV. Do not send the information to any person whose details you have been unable to separately verify.

V. Send the information as an encrypted document attached to an email. If you are unsure as to how to encrypt a file please speak to a member of the IT Team or your line manager.

VI. Provide the encryption key or password by a separate contact with the recipient(s) –preferably by telephone.

VII. Do not identify such information in the subject line of any email.

VIII. Request confirmation of safe receipt.

IX. When sending an email containing personal or sensitive data, the name of the individual must not be included in the subject line and the document containing the information must be encrypted.

X. To provide additional security you should put 'CONFIDENTIAL' in the subject line and as a header in the email and any attachments to the email.

9.14 **Students and email**

9.14.1 If students are issued with an e-mail account when joining the Trust, staff should make students aware of the following:

- Student email users are required to use appropriate formal language in their messages.
- Students should not reveal any personal details about themselves or others in email communication.
- Students should not use email to arrange to meet anyone.
- Students must ensure that any email attachments they receive are checked for viruses before opening.
- Students must immediately inform a teacher/trusted adult if they receive an offensive email.
- Staff should inform other relevant staff if they become aware of any student misuse of emails.

10. Use of phones

10.1 Staff must never give their personal phone numbers to parents or pupils, nor use their personal phone numbers to contact parents and carers.

10.2 Staff must always use phones provided by the school when contacting parents and carers.

10.3 Staff with personal devices who have been authorised to download the 3CX application may use their personal device to contact parents and carers however must ensure that the app is used and contact is therefore made via their office extension, not their personal mobile number.

10.4 Staff who are provided with mobile phones as equipment for their role must abide by the same rules for ICT acceptable use as outlined in this policy.

11. Monitoring of Trust networks and use of ICT facilities

11.1 Pathfinder Schools reserves the right to monitor the use of its ICT facilities and network. This includes, but is not limited to, monitoring of:

- Internet sites visited
- Bandwidth usage
- Email accounts
- User activity/access logs
- Any other electronic communications
- Only authorised staff may inspect, monitor, intercept, assess, record, and disclose the above, to the extent permitted by law.

11.2 Pathfinder Schools may monitor ICT use to:

- Obtain information related to its business
- Investigate compliance with Trust policies, procedures, and standards
- Ensure effective Trust, school, and ICT operation
- Conduct training or quality control exercises
- Prevent or detect crime
- Comply with a subject access request, Freedom of Information Act request, or any other legal obligation

12. Storage

12.1 All users are provided with storage space for their files on the Trust's servers.

12.2 This storage is provided on the understanding that:

- All data is stored in the approved area-Office 365 storage via OneDrive or SharePoint.
- Any data saved in areas other than approved locations may not be backed up by the IT team.
- Data is stored in line with the Trust's retention schedule (see Data Protection Policy)
- No inappropriate material is stored e.g. pornography or libellous material.
- No material is stored that infringes copyright i.e. illegal copies of any audio or video file or software program.
- No personal information about others is stored without direct reference to the Data Protection Act.
- Pathfinder Schools reserves the right to withdraw access to files and materials whose ownership is in question whilst an investigation is carried out.
- Users may not use the Trust's IT facilities or services to store personal non-work-related information or materials (such as music, videos, or photos).

13. Personal use

13.1 Staff are permitted to occasionally use Trust ICT facilities for personal use subject to certain conditions set out below. Personal use of ICT facilities must not be overused or abused.

13.2 Pathfinder Schools may withdraw permission for it at any time or restrict access at their discretion.

Personal use is permitted provided that such use:

- Does not take place during working time
- Does not constitute 'unacceptable use',
- Takes place when no pupils are present
- Does not interfere with their jobs, or prevent other staff or pupils from using the facilities for work or educational purposes
- Staff may not use the Trust's ICT facilities to store personal non-work-related information or materials (such as music, videos, or photos).

13.3 Staff should be aware that the use of Pathfinder Schools ICT facilities for personal use may put personal communications within the scope of the Trust's ICT monitoring activities.

13.4 Staff should be aware that personal use of ICT (even when not using Trust ICT facilities) can impact on their employment by, for instance putting personal details in the public domain, where pupils and parents could see them.

14. Internet

14.1 Pathfinder Schools provides access to the internet in as unrestricted a manner as possible on the understanding that:

- No user will access, download, store, bookmark, or record websites containing inappropriate content.
- No user will access websites containing online games or instant messaging services unless it has been an identified learning function which has been agreed by the Headteacher
- No user will attempt to access online shops or services whose age requirements they do not meet e.g. eBay or any other websites which are not relevant for work purposes.
- Visitors/contractors to Trust sites will not be permitted to use the Trust Wi-Fi unless specific authorisation is granted by the Headteacher or their designate through the provision of a guest Wi-Fi login. Where systems are not in place to offer a guest Wi-Fi login, advice should be sought from the Pathfinder Schools IT team, Wi-Fi codes should not be provided without discussing the details with the IT team.
- Authorisation will only be granted where access the Wi-Fi is required to fulfil the purpose of their visit (for instance, to access materials stored on personal devices as part of a presentation or lesson plan)
- Staff must not issue a Wi-Fi password to anyone who is not authorised to have it. Doing so could result in disciplinary action.

15. Software updates, firewalls, and anti-virus software

15.1 All Pathfinder Schools ICT devices that support software updates, security updates, and anti-virus products will be configured to perform such updates regularly or automatically.

15.2 Users must not circumvent or make any attempt to circumvent the administrative, physical, and technical safeguards we implement and maintain to protect personal data and the Trust's ICT facilities.

15.3 Any personal devices using the Trust's network must all be configured in this way.

16. Data protection and security

16.1 The Trust is responsible for making sure it has the appropriate level of security protection and procedures in place to safeguard its systems, staff and learners. It therefore takes steps to protect the security of its computing resources, data and user accounts. The effectiveness of these procedures is reviewed periodically to keep up with evolving cyber crime technologies.

16.2 Staff, pupils, parents/carers and others who use the school's ICT facilities should use safe computing practices at all times. We aim to meet the cyber security standards recommended by the Department for Education's https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges?utm_medium=email&utm_campaign=govuk-notifications-topic&utm_source=65a86d1d-7593-4f78-8e3c-6b4d3df15703&utm_content=immediately guidance on digital and technology standards in schools and colleges, including the use of:

- Firewalls
- Security features
- User authentication and multi-factor authentication
- Anti-malware software

17. Passwords

17.1 All users of the Trust's ICT facilities should set strong passwords for their accounts and keep these passwords secure.

17.2 Users are responsible for the security of their passwords and accounts, and for setting permissions for accounts and files they control.

17.3 Members of staff or pupils who disclose account or password information may face disciplinary action. Parents, visitors or volunteers who disclose account or password information may have their access rights revoked.

18. Encryption

18.1 Pathfinder Schools ensures that its devices and systems have an appropriate level of encryption.

18.2 Pathfinder Schools staff may only use personal devices to access Trust data, work remotely, or take personal data (such as pupil information) out of school if they have been specifically authorised to do so by the Headteacher/their line manager for Central Team staff.

18.3 Use of such personal devices will only be authorised if the devices have appropriate levels of security and encryption, as defined by the Pathfinder Schools ICT Manager.

19. Remote access

19.1 Pathfinder Schools supports its staff to access the Trust's facilities and materials remotely. Requests for remote access should be made to the ICT Team using the

Helpdesk system. This will be accommodated where possible and where authorised by an individual's line manager.

19.2 Staff accessing the Trust's ICT facilities and materials remotely must abide by the same rules as those accessing the facilities and materials on-site. Staff must be particularly vigilant if they use the school's ICT facilities outside the school and take such precautions as outlined in the Pathfinder Schools Homeworking guidance.

20. You are mindful of confidentiality if working from home or outside of the Trust premises. Ensure that no one else can see the screens when sending information and always lock your laptop when not working, even if it is only for a minute or two. Do not discuss students or Trust/school matters with anyone other than work colleagues and take care that you cannot be overheard.

20.1 Pathfinder Schools ICT facilities contain information that is confidential and/or subject to data protection legislation. Such information must be treated with extreme care and in accordance with our data protection policy.

30. **Protection from cyber attacks**

The Trust will:

- Ensure cyber security is given the time and resources it needs to make the Trust secure
- Provide annual training for staff (and include this training in any induction for new starters, if they join outside of the school's annual training window) on the basics of cyber security, including how to:
    - Check the sender address in an email
    - Respond to a request for bank details, personal information or login details
    - Verify requests for payments or changes to information
- Make sure staff are aware of its procedures for reporting and responding to cyber security incidents
- Investigate whether our IT software needs updating or replacing to be more secure
- Not engage in ransom requests from ransomware attacks, as this would not guarantee recovery of data
- Put controls in place that are:
    - **Proportionate**: the Trust will verify this using a third-party audit, currently Cyber Essentials, this is an annual process.
    - **Multi-layered**: everyone will be clear on what to look out for to keep our systems safe
    - **Up to date:** with a system in place to monitor when the school needs to update its software
    - **Regularly reviewed and tested**: to make sure the systems are as effective and secure as they can be
- Back up critical data daily and store these backups on the cloud.
- Delegate specific responsibility for maintaining the security of our management information system (MIS) to our cloud-based provider, presently Bromcom.

Decisions made regarding access and permissions is delegated to school based leaders,

- Make sure staff:
  - Dial into our network using a virtual private network (VPN) when working from home
  - Enable multi-factor authentication where they can, on things like school email accounts
  - Store passwords securely using a password manager
- Make sure ICT staff conduct regular access reviews to make sure each user in the Trust has the right level of permissions and admin rights
- Have a firewall in place that is switched on
- Check that its supply chain is secure, for example by asking suppliers about how secure their business practices are and checking if they have the Cyber Essentials certification
- Develop, review and test an incident response plan with the IT department including, for example, how the Trust will communicate with everyone if communications go down, who will be contacted and when, and who will notify Action Fraud of the incident. This plan will be reviewed and tested every six months and after a significant event has occurred, using the NCSC's 'Exercise in a Box'

21. **Internet Access**

21.1 The Trust's wireless internet connection is secure.

21.2 The Trust's WiFi arrangements included filtering, are managed differently for staff/pupils/parents or carers/members of the public with distinct access and permissions as defined by the Trust IT Team.

21.3 We recognise that filters aren't fool proof, if an inappropriate site is accessed which bypasses or is not identified by the filtered this should be reported to the IT Team who will ensure the site is blocked to prevent future access. Safeguarding protocols associated with the site should be followed by Safeguarding Leads.

21.4 Parents/carers and visitors

21.5 Parents/carers and visitors to the school will not be permitted to use the Trust's WiFi unless specific authorisation is granted by the headteacher or their designate.

21.6 The headteacher or their designate will only grant authorisation if:

21.7 Parents/carers are working with the school in an official capacity (e.g. as a volunteer or as a member of the PTA)

21.8 Visitors need to access the Trust's WiFi in order to fulfil the purpose of their visit (for instance, to access materials stored on personal devices as part of a presentation or lesson plan)

21.9 Staff must not give the WiFi password to anyone who is not authorised to have it. Doing so could result in disciplinary action.

22. The use of personal devices

22.1 A personal device may only be used for work purposes where written approval has been given by the Headteacher/Principal and the CEO for Central Team members. Further to written approval, the following conditions apply when using a personal device for work.

Android and iOS

- The device must be running the latest possible operating system version
- Only Office 365 apps are permitted to be used on an Android or an iOS device for work use
- All other resources can only be accessed via a web browser
- Username and passwords for work accounts must not be saved onto the local device or to any personal cloud account
- The device must be encrypted and have a passcode set
- All Office 365 apps should have a PIN set that is different from the passcode on the device
- No one else should know the PIN to the Office 365 apps
- When installing an Office 365 app staff accept the controls set by the Pathfinder Schools IT Department, this includes the ability to wipe company-owned data from the device.

Windows and other devices

- All resources and applications should be accessed via a web browser only
- No files should be downloaded to the device
- Software applications like Outlook, Teams, and other Office 365 applications should not be signed into and should only be used via a web browser
- Staff should not leave themselves signed in and should always sign out when they have finished working
- Username and passwords for work accounts must not be saved onto the local device or to any personal cloud account
- The user device must have the latest security updates installed and be running updated anti-virus and malware software

5.5 Monitoring and filtering of the Trust network and use of ICT facilities

To safeguard and promote the welfare of children and provide them with a safe environment to learn, the school reserves the right to filter and monitor the use of its ICT facilities and network. This includes, but is not limited to, the filtering and monitoring of:

- Internet sites visited
- Bandwidth usage
- Email accounts
- Telephone calls
- User activity/access logs
- Any other electronic communications

Only authorised personnel may filter, inspect, monitor, intercept, assess, record and disclose the above, to the extent permitted by law. The Trust utilises Netsweepet and Senso for filtering and monitoring purposes.

The Trust monitors ICT use in order to:

- Obtain information related to school business
- Investigate compliance with school policies, procedures and standards
- Ensure effective school and ICT operation
- Conduct training or quality control exercises
- Prevent or detect crime
- Comply with a subject access request, Freedom of Information Act request, or any other legal obligation

Our Trust is responsible for making sure that:

- The school meets the DfE's filtering and monitoring standards
- Appropriate filtering and monitoring systems are in place
- Staff are aware of those systems and trained in their related roles and responsibilities
    - For the leadership team and relevant staff, this will include how to manage the processes and systems effectively and how to escalate concerns
- It regularly reviews the effectiveness of the school's monitoring and filtering systems

The school's designated safeguarding lead (DSL) will take lead responsibility for understanding the filtering and monitoring systems and processes in place.

Where appropriate, staff may raise concerns about monitored activity with the school's DSL and ICT manager, as appropriate.

5.5 Monitoring and filtering of the school network and use of ICT facilities

To safeguard and promote the welfare of children and provide them with a safe environment to learn, the school reserves the right to filter and monitor the use of its ICT facilities and network. This includes, but is not limited to, the filtering and monitoring of:

- Internet sites visited
- Bandwidth usage
- Email accounts
- Telephone calls
- User activity/access logs
- Any other electronic communications

Only authorised ICT personnel may filter, inspect, monitor, intercept, assess, record and disclose the above, to the extent permitted by law.

The Trust monitors ICT use in order to:

- Obtain information related to school business
- Investigate compliance with school policies, procedures and standards
- Ensure effective school and ICT operation
- Conduct training or quality control exercises

Prevent or detect crime

- Comply with a subject access request, Freedom of Information Act request, or any other legal obligation

Our Trust Board is responsible for making sure that:

- The Trust meets the DfE's filtering and monitoring standards https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/filtering-and-monitoring-standards-for-schools-and-colleges
- Appropriate filtering and monitoring systems are in place
- Staff are aware of those systems and trained in their related roles and responsibilities
- For the leadership team and relevant staff, this will include how to manage the processes and systems effectively and how to escalate concerns
- It regularly reviews the effectiveness of the school's monitoring and filtering systems

The school's designated safeguarding lead (DSL) will take lead responsibility for understanding the filtering and monitoring systems and processes in place.

Where appropriate, staff may raise concerns about monitored activity with the school's DSL and Director of IT, as appropriate.

23. **Remote and blended learning**

23.1 In some cases, learning will be delivered exclusively online or as part of a blended approach depending on the circumstances of the school/academy or individual students.

23.2 Blended learning is an approach that combines classroom teaching with online and digital learning tools, ensuring continuity in student learning through the assistance of an online learning environment.

23.3 Guidance from the DfE https://www.gov.uk/government/publications/remote-education-goodpractice/remote-education-good-practice states:

I. Schools will signpost the relevant online safety advice for students and parents/carers available through the schools' website/other appropriate means.

II. Schools will ensure that students receive appropriate information and guidance about how to access and behave during remote learning sessions.

23.4 Guidance from the DfE https://www.gov.uk/government/publications/remote-education-goodpractice/remote-education-good-practice states:

The Education Endowment Foundation (EEF) has found that the effectiveness of remote teaching is determined by many of the same factors as determining the effectiveness of live classroom teaching. For example:

- ensuring pupils receive clear explanations
- supporting growth in confidence with new material through scaffolded practice
- application of new knowledge or skills
- enabling pupils to receive feedback on how to progress

23.5 Pathfinder Schools uses Microsoft 365 as the common platform to facilitate the online learning environment, details of how these are used by different members of the community are outlined in Table A on page 13 of this document.

23.6 By using a common approach provides us with a safe and consistent way to share content, including:

- Conducting live online lessons
- Posting pre-recorded video lessons
- Communicating with students and parents
- Setting assignments and engaging students in feedback
- Students interacting with add-on Apps

Table A

Microsoft 365 Suite	**Students**	**Teachers within a school**	**All schools' staff across Pathfinder Schools**	**Families and carers**
Microsoft Teams	Class Collaboration Peer Collaboration Assignments	Class Collaboration Professional Learning Student Assignments	Staff Collaboration Live Meetings	Regular email updates on students' learning
Outlook Email	Formal communication	Formal communications	Formal communication	Formal communications
Stream	Safe and secure video recordings	Safe and secure video recordings	Safe and secure video recordings	
OneDrive	Personal file-storage	Personal file-storage		
SharePoint	School and system websites	Shared file store School websites	Shared file store School and system websites	
Forms	Surveys, quizzes	Surveys, feedback tools	Surveys, feedback tools	Surveys, feedback tools
Learning Tools	Immersive Reader Microsoft Translator	Microsoft Translator for student and parent communications	Microsoft Translator for parent communication	Microsoft Translator for parent communications

23.7 All staff must engage with training for Microsoft Teams so that they are confident in using the basic features relating to communication, collaboration, and video calling.

23.8 To keep everyone safe, all online learning interactions between teachers and students must be channelled through Microsoft Teams. Communication via Teams would normally be in the school setting, where this is not possible, communication from home is allowed.

23.9 It is acknowledged that each school is at a different stage in the development of their online learning approach and may use other learning platforms (Purple Mash, Class Dojo) whilst they are supported in transitioning fully to Microsoft Teams. Schools may also opt to use a different platform for pupils in the early years, such as Seesaw.

23.10 It is important that all staff who interact with children, including online, continue to look out for signs a child may be at risk. Any such concerns should be dealt with as per the Child Protection Policy and where appropriate referrals should still be made to children's social care and as required, the police.

23.11 Online teaching should follow the same principles as set out in the Pathfinder Schools Code of Conduct.

24. Expectations and guidance for safe and effective online learning

24.1 The following expectations are intended to facilitate safe and effective online learning. These are an extension of the expectations for face-to-face learning.

24.2 At Pathfinder Schools, we will ensure:

- There is a nominated leader with responsibility for blended learning in our school;
- All relevant policies and procedures will be updated to incorporate a blended approach;
- Students and families are clear about how to report safeguarding concerns;
- Staff and tutors have up-to-date safeguarding training and know-how to report safeguarding concerns
- Staff and tutors are aware of the need for appropriate professional behaviours online

24.3 **Expectations for Staff and Tutors when using Microsoft Teams for Remote Online Lessons:**

- Expectations for online sessions should be shared and agreed upon in advance of the online session and must be adhered to.
- Staff/tutors must wear suitable professional clothing as if they were in school;
- Any devices used should be in appropriate areas (i.e. not bedrooms) and the background tool must be used to blur or change the background.
- Staff and students do not inappropriately use the chat function (this can be blocked within classes and by admin)

- The live class should be recorded so that if any issues were to arise, the video can be reviewed
- Live classes should be kept to a reasonable length of time to cover the curriculum content; Staff should also record, the length, time, date, and attendance of any online teaching sessions held
- Language must be professional and appropriate, including any family members in the background
- Staff/tutor should record the time, date, and attendance of any sessions held
- Staff/tutor hosts the meeting and remains in control of the meeting
- Staff must not join a meeting hosted by a parent or student
- Only staff may use the video/broadcasting functionality
- It is recommended that students switch off their microphones to limit issues and can use the chat functionality to ask questions. If it is deemed appropriate a student can activate their microphone but should be appropriate.
- Schools should consider carefully whether or not 1:1 teaching takes place, where it has been deemed appropriate and approved by the Headteacher the procedure outlined in Appendix 4 should be followed. This also applies to any 1:1 audio-only lesson.
- Safeguarding and pastoral staff may conduct 1:1 meetings and these must be recorded unless it compromises the student disclosing or other safeguarding protocols. A risk assessment must be completed in this situation, which must be signed by the Headteacher (or other delegated person), a Pro-forma risk assessment is available in Appendix 5 of this document.
- Although online assessment packages can be used it is important that the software is suitably age-restricted and that communication within those packages is kept to a minimum.
- All software used must be agreed to by the Headteacher (or person with delegated responsibility)
- External software must have relevant security measures in place and should for example meet industry standards. Personal information should be limited with these packages, for example, student log-in details should be numerical so that names and surnames, etc. are not shared.
- No user will access, download, store, bookmark, or record websites containing inappropriate content. It is also important that users do not direct students to websites that contain inappropriate content or have unsuitable age restrictions.
- Websites such as TikTok, Facebook, etc. are 13+ and YouTube is 13+ and 11+ with parental permission. All video links should be checked for age-appropriateness before distributing to students.

24.4 **Expectations for Staff and Tutors using Microsoft Teams when meeting with parents/carers:**

- In addition to the expectations outlined in 26.2 and 26.3;
- The teacher/staff member hosts the meeting and remains the leader of the meeting

- If the parent/carer or other attendee uses language that is considered inappropriate or aggressive the member of staff reserves the right to end the meeting
- All attendees will be advised of the meeting expectations and that the meetings will be recorded subject to consent.

24.5 Parents/carers will be asked to sign a copy of an agreement that outlines the expectations of a Teams meeting.

25. Reporting Online Safeguarding Concerns

25.0 We have all have a responsibility when it comes to online safety and needs to ensure the Trust's online procedures keep children and young people safe.

25.1 If you think a child is in immediate danger, contact the police on 999. If you're worried about a child but they are not in immediate danger, you should share your concerns with the Designated Safeguarding Lead and follow your school's child protection procedures.

25.2 Online abuse is any type of abuse that happens on the internet, facilitated through technology like computers, tablets, mobile phones, and other internet-enabled devices (Department for Education, 2018; Department of Health, 2017; Scottish Government, 2014; Welsh Assembly Government, 2018).

It can happen anywhere online that allows digital communication, such as:

- social networks
- text messages and messaging apps
- email and private messaging
- online chats
- comments on live streaming sites
- voice chat in games.

25.3 Children and young people can be revictimised (experience further abuse) when abusive content is recorded, uploaded, or shared by others online. This can happen if the original abuse happened online or offline.

25.4 Children and young people may experience several types of abuse online:

- bullying/cyberbullying
- emotional abuse (this includes emotional blackmail, for example pressuring children and young people to comply with sexual requests via technology)
- sexting (pressure or coercion to create sexual images)
- sexual abuse
- sexual exploitation

25.5 Reporting online child abuse images

- It's against the law to produce or share images of child abuse, even if the image was self-created. This includes sharing images and videos over social media. If you see a video or image that shows a child being abused:
- Don't comment, like, or share the video or image, as this will distribute it further

- Report it to the website you've seen it on
- Report it to the Designated Safeguarding Lead

26. **Social Media**

26.1 For this policy, the term social media is used to describe any type of interactive website or online platform/tool that allows parties to communicate or interact with each other in some way by sharing information, opinions, knowledge, and interests and to share data in a public forum or to participate in social networking, resulting in several different activities. This also includes some games, for example, Minecraft or World of Warcraft, and video sharing platforms such as YouTube which have social media elements to them.

Social Media activities include, but are not limited to:

26.1.1 Maintaining a profile page on social / business networking sites such as Facebook, YouTube, LinkedIn, Twitter, Instagram, Tiktok, Reddit, SnapChat, Wikipedia , WhatsApp, Vine ,Tumblr ,Tinder, Grindr, Pinterest, and all other social networking sites, internet postings and blogs, creating posts and/or stories videos and reels.

- Writing or commenting on a blog, whether it is your own or the blog of another person / informational site.
- Use of social medial for business purposes as well as personal in a manner that may affect Pathfinder Schools.
- Taking part in discussions on web forums or message boards such as YouTube
- Leaving product or service reviews on business websites or customer review websites
- Taking part in online polls.
- Uploading multimedia on networking sites such as YouTube, Instagram, WhatsApp, Twitter, and Tumblr.
- Liking, re-tweeting, and commenting on posts of your own, another person, or other social media account.
- Games that have an online chat or interaction function

26.2 Many other forms of social media also exist which may not be listed in this Policy, however, individuals should be aware that this is area is constantly evolving and they are reminded of their continued responsibility to keep up to date with developments and review their privacy settings regularly when using social media sites.

26.3 **The use of social media**

27. Personal use of social media is never permitted during working hours or by means of our computers, networks and other IT resources and communications systems.

27.1.1 Pathfinder Schools recognise that employees will use social media in a personal capacity and the Trust actively encourages colleagues to find creative ways to use social media to promote the Trust, their school and to innovate in new ways for our pupils to learn.

27.1.2 There are risks associated with social media use, especially around the issues of safeguarding, bullying, and personal reputation. This document aims to encourage the safe use of social media.

27.1.3 Employees must understand that they are personally responsible for all comments, images, or information that they post online, this applies to personal communication. Therefore, all employees must ensure that when posting any information, images, or making comments, they do not:

- Bring the Trust into disrepute. e.g., by making derogatory or defamatory comments, either directly or indirectly, about the Trust, school, colleagues, individuals, pupils, or parents, etc. that could negatively impact the Trust's reputation or cause embarrassment. This includes posting images or links to inappropriate content or using inappropriate language.

- Breach confidentiality. e.g., revealing confidential information owned by Pathfinder Schools relating to its activities, finances, employees, or pupils.

- Undertake any Behaviour which may be considered discriminatory, or as bullying and/or harassment of any individual. e.g., making offensive or derogatory comments (either directly or indirectly) relating to sex, gender, race, disability, sexual orientation, religion, belief, or age; using social media to bully ("Cyberbullying") another individual; or posting images that are discriminatory or offensive or linking to such content.

27.2 As with all personal internet use, employees using social media sites must also observe the specific requirements of the documents named at the beginning of this policy.

27.3 **Training and engagement with staff**

27.3.1 Pathfinder Schools will:

- Provide this policy to all individuals engaged by the Trust as part of induction and will encourage ongoing open and transparent conversations about social media use.
- Provide up-to-date and appropriate training regularly, with at least annual updates. This will be done through stand-alone sessions or drip-feeding with small sessions/ bulletin reminders.
- Recognise the expertise staff build by undertaking safeguarding training and managing safeguarding concerns and provide opportunities for staff to contribute to and shape online/ICT/social media safety policies and procedures.
- Make staff aware that our IT systems are monitored, and that activity can be traced to individual users; staff will be reminded to behave professionally and in accordance with our policies when accessing our systems and devices.
- Make staff aware that their online conduct outside of the setting, including personal use of social media, could have an impact on their professional role and reputation.

- Ensure all members of staff are aware of the procedures to follow regarding online safety concerns affecting learners, colleagues, or other members of the Trust community.

27.4 **Employee responsibilities**

27.4.1 Employees are personally responsible for the content that they publish on social media, including "Likes" (on Facebook)/ "re-tweets" (on Twitter), Snapchat, Instagram, LinkedIn, WhatsApp, TikTok, etc. Employees should assume that everything that is written is permanent and can be viewed by anyone at any time. It is fair and reasonable to take disciplinary action against employees for inappropriate use of social media, including the use of social media conducted outside of working hours.

27.4.2 Individuals must observe and note the following listed guidance (which is not exhaustive);

- Individuals should assume that everything can be traced back to them personally as well as to their colleagues, Pathfinder Schools, their school, pupils and parents.

- Be respectful to others when making any statement on social media and be aware that you are personally responsible for all communications which will be published on the internet for anyone to see.

- If you see social media content that disparages or reflects poorly on us, you should contact your line manager at the earliest opportunity.

- If you are uncertain or concerned about the appropriateness of any statement or posting, refrain from posting it until you have discussed it with your manager.

- If you disclose your affiliation with us on your profile or in any social media postings, you must state that your views do not represent those of your employer (unless you are authorised to speak on our behalf). You should also ensure that your profile and any content you post are consistent with the professional image you present to Trust stakeholders and colleagues.

- To avoid any conflict of interest and to meet the expectations outlined in the Code of Conduct employees must ensure that personal social networking sites are set to private, and pupils and parents/carers/pupil family members are never listed as approved contacts. Approaches from the aforementioned via social media must be disclosed to an appropriate senior leader without delay.

- Information must not be posted that would disclose the identity of pupils or could in any way be linked to a pupil(s). This includes photographs or videos of pupils or their homes.

- You should make it clear in social media postings, or in your personal profile, that you are speaking on your own behalf. Write in the first person and use a personal email address.

- Pupils must not be discussed on social media sites.

- Individuals should not post information on sites including photographs and videos that could bring Pathfinder Schools into disrepute.
- Individuals must not represent their views/opinions as being those of Pathfinder Schools.
- Individuals must not divulge any information that is confidential to Pathfinder Schools or a partner organisation.
- Potentially false, derogatory, offensive, or defamatory remarks directly or indirectly towards Pathfinder Schools, its employees, pupils, pupils' relatives, the school suppliers, and partner organisations should not be posted on social media sites.
- Individuals must ensure content or links to other content do not interfere with their work commitments or be on inappropriate content.
- Individuals must not either endorse or criticise service providers used by Pathfinder Schools or develop online relationships which create a conflict of interest.
- Individuals must not upload, post, forward or post a link to any pornographic material (that is, writing, pictures, films, and video clips of a sexually explicit or arousing nature).
- When posting on social media sites Individuals must observe the requirements of the Equality Act and the Human Rights Act and must not use any offensive, obscene, derogatory, discriminatory language which may also cause embarrassment to the Trust and its, employees, pupils, pupils' relatives, suppliers and partner organisations.
- Individuals must never impersonate another person.
- Individuals must not upload~~,~~ forward, or post a link that is likely to: create any liability for the School (whether criminal or civil), breach copyright law or other affect intellectual property rights, or which invades the privacy of any person.
- All Individuals are advised to safeguard themselves and their privacy when using social media sites. Advice will be provided to staff via staff training and by sharing appropriate guidance and resources regularly. This will include (but is not limited to):
    - Setting the privacy levels of their sites.
    - Being aware of location sharing services.
    - Opting out of public listings on social networking sites. o Logging out of accounts after use.
    - Keeping passwords safe and confidential.
    - Ensuring staff do not represent their personal views as that of the setting.

27.5 **Disciplinary action**

27.5.1 Individuals should be aware that the use of social media sites in a manner contrary to this policy, including if others implicate you in a breach of any of the points listed within this document may result in disciplinary action and serious cases may be treated as gross misconduct, which itself could lead to summary dismissal.

27.5.2 In certain circumstances, such misuse may constitute a criminal offence or otherwise give rise to legal liability against employees and the Trust. Such cases will be referred to the police.

27.5.3 Individuals who become aware of any use of social media by other members of staff in breach of this guidance must report the matter to the Headteacher.

27.5.4 Individuals should be mindful when placing information on social media sites that this information is visible to a large audience and could identify where they work and with whom, thereby increasing the opportunity for identifying fraud, false allegations, and threats. In addition, it may be possible through social media sites for children or vulnerable adults to be identified, which could have implications for their security. Individuals should therefore be mindful that they:

- Do not reveal personal or private information about themselves such as date of birth, address details and bank details, etc. Posting such information could increase the risk of identity theft.
- Remember that there is the scope for causing offence or unintentionally causing embarrassment, for example, if pupils find photographs of their teacher which may cause embarrassment and/or damage to professional reputation and that of Pathfinder Schools.
- Be mindful that posting images, comments, or joining online campaigns may be viewed by colleagues, parents, ex-pupils, etc.
- Ensure that where you do post comments make a clear statement that any comments expressed are your own and not those of Pathfinder Schools.
- Finally, consideration should be given to the information posted on social media sites, and employees are advised to use appropriately the security settings on such sites to assist in limiting the concerns above.

27.6 **Monitoring the use of social media sites**

27.6.1 Individuals should be aware that any use of social media websites (whether or not accessed for work purposes) may be monitored and, where breaches of this Guidance are found, action may be taken under the Disciplinary policy.

27.6.2 Pathfinder Schools considers that valid reasons for checking an individuals internet usage include suspicions that the employee has:

- been using social media websites when they should be working; or
- acted in a way that is in breach of the rules set out in this policy.

27.7 **Trust/School social media accounts**

27.7.1 The Trust and individual schools have official social media pages, managed by nominated personnel. The Trust has guidelines for what can and cannot be posted on its social media accounts. Those who are authorised to manage the account must ensure they abide by these guidelines at all times.

27.7.2 Senior leaders should act as the point of contact for requests from staff to set up professional social media accounts and should approve or decline these requests.

27.7.3 Staff who wish to set up or manage an existing professional social media account must complete an application (Appendix 3) and submit it to an appropriate senior leader. No further action should be taken until written approval has been given.

27.7.4 Staff who are nominated to manage professional accounts are responsible for creating the accounts, storing account details and logins securely, and not sharing log-in details with unauthorised staff.

27.7.5 Staff members who have not been authorised to manage, or post to, the account, must not access, or attempt to access the account.

27.8 **Monitoring**

27.8.1 Trust/School accounts will be monitored daily by the designated person with responsibility for media accounts. Any comments, queries, or complaints made through these accounts must be responded to within 24 hours (or on the next working day if received at a weekend) even if the response is only to acknowledge receipt. Daily monitoring and intervention are essential in case a situation arises where bullying or any other inappropriate behaviour arises on a school social media account.

27.9 **Expectations**

- The Trust requires that all users using social media adhere to the standard of behaviour as set out in this policy and other relevant policies.
- School/Trust social media accounts must not be used for personal gain. Individuals must ensure that confidentiality is maintained on social media even after their relationship with the Trust comes to an end.
- Users must declare who they are in social media posts or accounts. Anonymous posts are not permitted concerning Trust activity.
- If a journalist makes, contact about posts made using social media staff should notify a senior leader who will contact the Central Team to seek advice.
- Users of social media should consider the copyright of the content they are sharing and, where necessary, should seek permission from the copyright holder before sharing.

27.10 **Tone**

27.10.1 The tone of content published on social media on behalf of the Trust should be appropriate to the audience, whilst retaining appropriate levels of professional standards.

27.10.2 **Our tone of voice should:**

- always embody and express our values, of collaboration, humanity, and independence
- always sound clear, helpful, optimistic, and polite
- be sincere and personal, in a style that imagines we are talking to our audience
- we should always aim to write engaging informative content that gets the message across in a friendly way
- Use shorter words
- Use everyday English, avoiding jargon wherever possible
- Use active verbs as much as possible – 'we will do it rather than 'it will be done by us'

27.11 **Managing school social media accounts**

The Do's

- Check with a senior leader before publishing content that may have controversial implications for the Trust
- Use an appropriate and professional tone as outlined in section 28.13 of this document
- Be respectful to all parties
- Ensure you have permission to 'share' other peoples' materials and acknowledge the author
- Express opinions but do so in a balanced and measured manner
- Think before responding to comments and, when in doubt, get a second opinion
- Seek advice and report any mistakes using the school's/trust reporting process
- Consider turning off tagging people in images where possible

The Don'ts

- Don't make comments, post content, or link to materials that will bring the trust into disrepute
- Don't publish confidential or commercially sensitive material
- Don't breach copyright, data protection, or other relevant legislation
- Consider the appropriateness of content for any audience of trust accounts, and don't link to, embed, or add potentially inappropriate content
- Don't post derogatory, defamatory, offensive, harassing, or discriminatory content
- Don't use social media to air internal grievances

27.12 **Use of images**

27.12.1 Trust use of images can be assumed to be acceptable, providing the following guidelines are strictly adhered to;

- Permission to use any photos or video recordings should always be sought
- If anyone, for any reason, asks not to be filmed or photographed then their wishes should be respected.
- Schools should hold a list of pupils who cannot be photographed and this should be checked annually to ensure it is up to date. Under no circumstances should staff share or upload student pictures online other than via school-owned social media accounts

- Individuals should exercise their professional judgement about whether an image is appropriate to share on trust social media accounts. Students should be appropriately presented, not be subject to ridicule, and must not be on any school list of children whose images must not be published.

Appendix 1

Social media quick guide for staff

Guidance for Pathfinder Schools colleagues to use social media safely:

- Change your display name – use your first and middle name, use a maiden name, or put your surname backwards instead
- Change your profile picture to something unidentifiable, or if not, ensure that the image is professional
- Check your privacy settings regularly
- Be careful about tagging other staff members in images or posts
- Don't share anything publicly that you wouldn't be just as happy showing to pupils
- Don't use personal social media sites during school hours
- Don't make comments about your job, your colleagues, our school, pupils, contractors, service providers, or stakeholders online – once it's out there, it's out there
- Don't link your work email address to your social media accounts. Anyone who has this address (or your personal email address/mobile number) can find you using this information
- Consider uninstalling social media apps from your phone. The app recognises Wi-Fi connections and makes friend suggestions based on who else uses the same Wi-Fi connection (such as parents or pupils)

Check your privacy settings

Change the visibility of your posts and photos to 'Friends only', rather than 'Friends of friends'. Otherwise, pupils and their families may still be able to read your posts, see things you've shared, and look at your pictures if they're friends with anybody on your contacts list

Don't forget to check your old posts and photos – go to bit.ly/2MdQXMN to find out how to limit the visibility of previous posts on Facebook.

The public may still be able to see posts you've 'liked', even if your profile settings are private because this depends on the privacy settings of the original poster

Remember that some information is always public; your display name, profile picture, cover photo, user ID (in the URL for your profile), country, age range, and gender

What to do if…

A pupil adds you on social media:

- Without exception decline the request and block the pupil from viewing your profile
- Notify the senior leadership team or the Headteacher in writing (email is acceptable)
- Check your privacy settings again, and consider changing your display name or profile picture
- If the pupil asks you about the friend request in person, tell them that you're not allowed to accept friend requests from pupils, inform the senior leadership team or Headteacher without delay.

A parent/pupil relative adds you on social media:

- Without exception decline the request and block the parent from viewing your profile
- Notify the senior leadership team or the Headteacher in writing (email is acceptable)
- Check your privacy settings again, and consider changing your display name or profile picture
- If the parent asks you about the friend request in person, explain that you are prohibited from accepting requests from parents for safeguarding reasons, inform the senior leadership team or Headteacher in writing without delay. (email is acceptable)

You're being harassed on social media:

- Do not retaliate or respond in any way
- Save evidence of any abuse by taking screenshots and recording the time and date it occurred
- Report the material to r the relevant social network and ask them to remove it
- If the perpetrator is a current pupil or staff member, our pupil behaviour and disciplinary procedures are usually sufficient to deal with online incidents
- If the perpetrator is a parent/pupil relative or another external adult, a senior member of staff should invite them to a meeting to address any reasonable concerns or complaints and/or request they remove the offending comments or material
- If the comments are racist, sexist, of a sexual nature, or constitute a hate crime, you or a senior leader should consider contacting the police

Appendix 2i

Acceptable use agreement for adults engaged by Pathfinder Schools including staff, governors, trustee's, volunteers, and visitors

Acceptable use
Name of individual: **Position of individual** **Workplace location of the individual**
I understand that I must use the Trust's ICT facilities responsibly, to ensure that there is no risk to my safety or the safety and security of the systems, other users, and students. I recognise the value of the use of digital technology for enhancing learning and will ensure that students receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people. In addition to adhering to the Acceptable Use Policy detailed above and the Trust's Code of Conduct, I will comply with the below code of conduct which has been developed to ensure my professional and personal safety when delivering online learning.
For my professional and personal safety: • I understand and accept that the Trust will fully monitor my use of the school's digital technology and communications systems. • I understand that if my activity causes concern, safeguarding software installed across the Trust may automatically alert appropriate safeguarding specialists who may choose to investigate depending on the content of the alert. • I understand that the rules set out in this agreement also apply to the use of Trust-provided IT technologies (e.g. laptops, email, data, etc.) out of school, and to the transfer of personal data (digital or paper-based) out of school.

- I will always lock or sign out of any device I am not actively using or will be left unattended.
- If I choose to use my personal mobile telephone or another device to access Trust or Academy IT systems such as email or Office 365 apps including Teams, I will ensure that adequate security is in place such as a device password, Touch ID, or Face ID.
- I will immediately report any illegal, inappropriate, or harmful material or incident I become aware of, my line manager or appropriate person.
- I will immediately report potential data breaches to the Headteacher/Data Protection lead contact at my workplace.
- I will only use equipment that is provided by the Trust for teaching and school-related activities.
- I understand that if I leave the Trust, all my digital accounts will be suspended and my data deleted at the Trust's discretion.

I will be professional in my communications and actions when using Trust systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will professionally communicate with others, I will not use aggressive or inappropriate language.
- I will ensure that when I take and/or publish images of others I will do so with their permission and by the Trusts GDPR policy guidance on consent for digital/video images. I will not use my personal equipment to record these images unless I have permission to do so.
- If I am responsible for updating social networking sites on behalf of the school, I will do so following the school's policies and site guidance.
- I will only communicate with students and parents/carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any online activity that may compromise my professional responsibilities. This includes canvassing, lobbying, advocacy, or personal endorsement that has not been ratified by the Trust.
- All information discussed or received of a sensitive or confidential nature will remain so and only be discussed with relevant key staff such as the Headteacher or DSL.

Ensuring safe and secure access to technologies:

- When I use my personal digital device (e.g. personal laptop/tablets/phones) at home, I will follow the rules set out in this agreement and need to ensure that I am using the device on a secure network and that they are protected by up to date security patches and anti-virus software and are free from viruses.
- I will not use personal email addresses for academy/Trust-IT services nor register for any services on behalf of the Trust
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity

of the email (due to the risk of the attachment containing viruses or other harmful programmes) I will contact the IT team for advice.

- I will ensure that I place my data in my approved areas or a shared area if appropriate and I have been given access. If I house data anywhere else other than these approved locations I understand that the Trust IT service will not back it up and I will take responsibility for backing up any such data.
- I will not house any personal data on any Trust system.
- I will not try to upload, download or access any materials which are illegal (any data covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others.
- I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will not install or attempt to install programmes of any type on a machine or store programmes on a computer, nor will I try to alter computer settings, unless I have been permitted to.
- I will not try to use any applications, such as VPN, that might allow them to bypass the filtering/security systems in place to provide a safe learning and teaching environment.
- I will not disable or cause any damage to Trust equipment, or any equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the Trust Data Protection GDPR Policy. Where digital personal data is transferred outside the secure local network, you must take the necessary steps to ensure that the data is shared securely by either encrypting, password-protected, or the use of Office365. Paper-based protected and restricted data must be held in lockable storage.
- I understand that GDPR law requires that any staff or student data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by Trust policy to disclose such information to an appropriate authority
- I will immediately report any damage or faults involving equipment or software, however, this may have happened.
- I will not share my personal email address or phone number with students or parents

Use of copyright resources:

- I will ensure that copyright resources are only used or shared with appropriate permissions.
- Copyrighted work will not be downloaded or shared including music and videos unless an exemption applies for teaching purposes.
- These purposes include:
  ○ the copying of works in any medium as long as the use is solely to illustrate a point, it is not done for commercial purposes, it is accompanied by a sufficient acknowledgement, and the use is fair dealing. This means minor uses, such as displaying a few lines of poetry on an interactive whiteboard, are permitted but uses that would undermine sales of teaching materials are not;

○ performing, playing, or showing copyright works in a school, university, or another educational establishment for educational purposes. However, it only applies if the audience is limited to teachers, pupils, and others directly connected with the activities of the establishment. It will not generally apply if parents are in the audience. Examples of this are showing a video for English or drama lessons and the teaching of music. It is unlikely to include the playing of a video during a wet playtime purely to amuse the children; ○ by recording a TV programme or radio broadcast for non-commercial educational purposes in an educational establishment, provided there is no licensing scheme in place. Generally, a license will be required from the Educational Recording Agency; ○ making copies by using a photocopier, or similar device on behalf of an educational establishment for non-commercial instruction provided that there is no licensing scheme in place. Generally, a license will be required from the Copyright Licensing Agency. These and other, exemptions to copyright are listed here: https://www.gov.uk/guidance/exceptions-to-copyright
When using the internet in my professional capacity or for school-sanctioned personal use: • I will ensure that I have permission to use the original work of others in my work • Where work is protected by copyright, I will not download or distribute copies (including music and videos).
I have read and understood the above and agree that: • I am responsibly upholding the requirements laid out above at all times and that even while in personal time I am representing the values and integrity of the Trust. • I understand that this Acceptable Use Policy applies not only to my work and use of Trust digital technology equipment in my workplace, but also applies to my use of Trust systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by Trust • I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action in line with the Trust's Disciplinary Policy

Signed:	Date:

Completed forms should be returned electronically to (insert the appropriate point of contact)

Appendix 2ii

Acceptable use of the internet: agreement for parents and carers

Acceptable use of the internet: agreement for parents and carers	
Name of parent/carer: **Name of child:**	
Online channels are an important way for parents/carers to communicate with, or about, our school. The Trust uses the following channels: ➢ Our official Facebook pages ➢ Email/text groups for parents (announcements and information) ➢ Our management information system Bromcom Parents/carers also set up independent channels to help them stay on top of what's happening in their child's class. For example, class/year Facebook groups, email groups, or chats (through apps such as WhatsApp).	
When communicating with the school via official communication channels, or using private/independent channels to talk about the school, I will: • Be respectful towards members of staff, and the school, at all times • Be respectful of other parents/carers and children • Direct any complaints or concerns through the school and trust's official channels, so they can be dealt with in line with our complaints procedure I will not: • Use private groups, the school's Facebook page, or personal social media to complain about or criticise members of staff. This is not constructive and the school and Trust can't improve or address issues unless they are raised in an appropriate way • Use private groups, the school's Facebook page, or personal social media to complain about, or try to resolve, a behaviour issue involving other pupils. I will contact the school and speak to the appropriate member of staff if I'm aware of a specific behaviour issue or incident • Upload or share photos or videos on social media of any child other than my own, unless I have the permission of the other children's parents/carers	
Signed:	**Date:**

Acceptable use policy for EYFS & Key Stage 1 pupils

My name is	
	Tick, please
I only USE devices or apps, sites, or games if a trusted adult says so	
I ASK for help if I'm stuck or not sure	
I TELL a trusted adult if I'm upset, worried, scared, or confused	
If I get a FUNNY FEELING in my tummy, I talk to an adult	
I look out for my FRIENDS and tell someone if they need help	
I KNOW people online aren't always who they say they are	
Anything I do online can be shared and might stay online FOREVER	
I don't keep SECRETS or do DARES AND CHALLENGES just because someone tells me I have to	
I don't change CLOTHES or get undressed in front of a camera	
I always check before SHARING personal information	
I am KIND and polite to everyone	
I will not share my PASSWORDS with others	

My trusted adults are: _____ at school _____ at home

For parents/carers

We ask all children to sign an age-appropriate Acceptable Use of Technology Policy, which is a document that outlines who we expect them to behave when they are online and/or using technology.

Please read and discuss this agreement with your child and then sign it. If you have any questions or concerns please speak to [add name/job title]. You can find support and online safety resources for parents at https://www.thinkuknow.co.uk

Parent name	

Parent signature	
Date signed	

Appendix 2iii

Acceptable Use of Technology Policy for Key Stage 2 Students

These statements can keep me and others safe and happy at school and home;

1. I learn online – I use the school's internet, devices and logons for schoolwork, homework and other activities to learn and have fun. All school devices and systems are monitored, including when I'm using them at home.

2. I learn even when I can't go to school because of coronavirus – I don't behave differently when I'm learning at home, so I don't say or do things I wouldn't do in the classroom or nor do teachers or tutors. If I get asked or told to do anything that I would find strange in school, I will tell another teacher or a grown-up at home.

3. I ask permission – At home or school, I only use the devices, apps, sites, and games I am allowed to and when I am allowed to.

4. I am creative online – I don't just spend time on apps, sites, and games looking at things from other people. I get creative to learn and make things.

5. I am a friend online – I won't share or say anything that I know would upset another person or they wouldn't want to be shared. If a friend is worried or needs help, I remind them to talk to an adult, or even do it for them.

6. I am a secure online learner – I keep my passwords to myself and reset them if anyone finds them out. Friends don't share passwords!

7. I am careful what I click on – I don't click on unexpected links or popups, and only download or install things when I know it is safe or has been agreed by trusted adults. Sometimes app add-ons can cost money, so I must always check.

8. I ask for help if I am scared or worried – I will talk to a trusted adult if anything upsets me or worries me on an app, site, or game – it often helps. If I get a funny feeling, I talk about it.

9. I know it's not my fault if I see or someone sends me something bad – I won't get in trouble, but I mustn't share it. Instead, I will tell a trusted adult. If I make a mistake, I don't try to hide it but ask for help.

10. I communicate and collaborate online – with people I already know and have met in real life or that a trusted adult knows about.

11. I know new online friends might not be who they say they are – I am careful when someone wants to be my friend. Unless I have met them face to face, I can't be sure who they are.

12. I check with a parent/carer before I meet an online friend the first time; I never go alone.

13. I don't do live videos (live streams) on my own – and always check if it is allowed. I check with a trusted adult before I video chat with anybody for the first time.

14. I keep my body to myself online – I never get changed or show what's under my clothes when using a device with a camera. I remember my body is mine and no one should tell me what to do with it; I don't send any photos or videos without checking with a trusted adult.

15. I say no online if I need to – I don't have to do something just because someone dares or challenges me to do it, or to keep a secret. If I get asked anything that makes me worried, upset, or just confused, I should say no, stop chatting and tell a trusted adult immediately.

16. I tell my parents/carers what I do online – they might not know the app, site, or game, but they can still help me when things go wrong, and they want to know what I'm doing.

17. I follow age rules – 13+ games and apps aren't good for me so I don't use them – they may be scary, violent, or unsuitable. 18+ games are not more difficult or skills but very unsuitable.

18. I am private online – I only give out private information if a trusted adult says it's okay. This might be my address, phone number, location, or anything else that could identify me or my family and friends; if I turn on my location, I will remember to turn it off again. I do not keep secrets that are unsafe.

19. I am careful what I share and protect my online reputation – I know anything I do can be shared and might stay online forever (even on Snapchat or if I delete it).

20. I am a rule-follower online – I know that apps, sites, and games have rules on how to behave, and some have age restrictions. I follow the rules, block bullies, and report bad behaviour, at home and school.

21. I am not a bully – I do not post, make or share unkind, hurtful, or rude messages/comments and if I see it happening, I will tell my trusted adults.

22. I am part of a community – I do not make fun of anyone or exclude them because they are different from me. If I see anyone doing this, I tell a trusted adult and/or report it.

23. I respect people's work – I only edit or delete my digital work and only use words, pictures, or videos from other people if I have their permission or if it is copyright-free.

24. I am a researcher online – I use safe search tools approved by my trusted adults. I know I can't believe everything I see online, know which sites to trust, and know-how to double-check the information I find. If I am not sure I ask a trusted adult.

25. I know that the computer knows what I am typing and will report it to an adult if it is not safe.

I have read and understood this agreement.

If I have any questions, I will speak to a trusted adult at school that includes _____ Outside school, my trusted adults are_____

My trusted adults are: _____ at school _____ at home

For parents/carers

We ask all children to sign an age-appropriate Acceptable Use of Technology Policy, which is a document that outlines who we expect them to behave when they are online and/or using technology.

Please read and discuss this agreement with your child and then sign it. If you have any questions or concerns please speak to [add name/job title]. You can find support and online safety resources for parents at https://www.thinkuknow.co.uk

Parent name	
Parent signature	
Date signed	

Acceptable Use of Technology Policy for Key Stage 3-5 Students

We ask all young people and adults to sign an Acceptable Use of Technology Policy, which is a document that outlines who we expect them to behave when they are online and/or using school networks, connections, internet connectivity, and devices, cloud platforms, and social media (both when on the academy site and outside).

We understand the importance of children and young people being able to use the internet for education and personal development. This includes social media platforms, games, and apps. We aim to support children and young people in making use of these in our work. However, we also recognise that safeguards need to be in place to ensure children are kept safe at all times.

Ensuring student safety online is a partnership between the student, their parents/carers, and school, and all have a role to play in it and need to work together. This agreement is part of our overarching code of behaviour for children and young people and staff and volunteers. If you would like to know more about this, please speak to your tutor or classroom teacher. More information about online safety for parents is available from

More information about online safety for parents is available from;

- https://www.ceop.police.uk/safety-centre/
- https://www.thinkuknow.co.uk/
- https://educateagainsthate.com/parents/
- https://nationalonlinesafety.com/guides
- https://www.nspcc.org.uk/keeping-children-safe/online-safety/
- https://www.childline.org.uk/info-advice/bullying-abuse-safety/online-mobile-safety/sexting
- https://www.internetmatters.org/
- https://www.net-aware.org.uk/
- https://www.childnet.com/resources/

Websites such as TikTok, Facebook, etc. are 13+ and YouTube is 13+ and 11+ with parental permission. Please find out more about this at https://nationalonlinesafety.com/guides.

Please be aware that staff may direct students between the ages of 11 and 13 to YouTube videos for learning. These will be age-appropriate in content and by signing this agreement you are giving parental permissions for this.

More information about online safety for children and young people is available from

- https://www.thinkuknow.co.uk/

- https://www.childline.org.uk/info-advice/bullying-abuse-safety/online-mobile-safety/
- https://www.ceop.police.uk/safety-centre

Students: please read the following agreement and discuss it with your parents/carers.

Parents/carers: please read and discuss this agreement with your child and then sign it, then ask your child to sign it. If you have any questions or concerns, please speak to your child's tutor or classroom teacher.

Young person's agreement

1. I will treat myself and others with respect at all times. When I am online or using any device I will treat everyone as if I were talking to them face to face.

2. I will be responsible for my behaviour when using the internet, including social media platforms, games, and apps. This includes the resources I access; the language I use and the information I share.

3. I will try to be positive and creative to learn and share, develop new skills, and have fun. I will make sure my use of technology does not harm anyone else.

4. I will only access age-appropriate websites, social media platforms, games, and apps that are for school use.

5. I will not download copyrighted material (e.g. music, text, video, etc.).

6. It can be hard to stop using technology sometimes. I will try to use it in moderation and not let it affect other areas of my life (such as sleep).

7. I will consider my online reputation with everything I post and share – I know anything I do can be shared and might stay online forever (even if I delete it).

8. I will not deliberately browse, download or upload material that could be considered offensive or illegal. This includes sites that encourage hate or discrimination. If I accidentally come across any such material I will report it immediately to the school. If I am not in school I will inform my parent/carer.

9. I will not send anyone material that could be considered threatening, bullying, offensive, or illegal. Cyberbullying (along with all bullying) will be taken extremely seriously.

10. I will never take secret videos, photos, or recordings of teachers or students, including during remote learning.

11. I will not give out any personal information online, such as my name, phone number, or address.

12. I will not reveal my login, ID's, or passwords to anyone and change them regularly. If someone else knows my passwords I will tell a teacher.

13. I will not arrange a face-to-face meeting with someone I meet online unless I have discussed this with my parents/carers and am accompanied by a trusted adult.

14. If I am concerned or upset about anything I see on the internet or any messages that I receive, I know I can talk to a trusted adult. In school, this might be [enter name].

15. I understand that my internet use at [Name of school] will be monitored and logged and can be made available to the school.

16. I will not try to bypass online security in any or access any hacking files or tools. This is a criminal activity.

17. I will only access my documents and files and not try to view, change or delete other people's files or user areas without their permission.

18. When learning remotely using Teams, teachers and staff will not behave any differently to when we are in school. I will do the same.

19. I will only use personal devices in school if I have permission to do so.

20. I understand that it is illegal to possess, distribute, show, and making indecent images of children, this includes printing and viewing or 'downloading'. I understand that staff can search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads, and other tablet devices, where they believe there is a 'good reason' to do so.

21. I understand that the computer systems are recording the keystrokes that I am typing. This will be reported to an adult if it is not safe.

Online Learning (Microsoft Teams)

Pathfinder Schools uses Microsoft Teams as the learning platform providing communication to staff classes and student groups.

I agree that:

• I will use Microsoft Teams and other authorised websites to complete learning activities.

• I will ensure that all work uploaded or files sent will be appropriate.

• I will only use the chat function to contact my teacher if I need help with the work set. If this is required I understand that this needs to be appropriate.

• I will limit the use of the chat functionality with other students, and when used will make sure that it is appropriate as records are kept of all chats.

• I will not use the video functionality. If needed, and requested by a member of staff, I can activate my microphone to talk but must be appropriate.

• I understand that lessons/video communication is recorded for safety. I understand that these rules are designed to keep me safe and that if I choose not to follow them, school staff may contact my parents/carers

Signatures: We have discussed this online safety agreement and agree to follow the rules set out above.

Parent name		Student name	
Parent signature		Student signature	
Date signed		Date signed	

Appendix 2v

Agreement for Parents/Carers when enabling Microsoft Teams learning in the home:

1. I will remind my child about their Acceptable Use and Remote learning agreements.
2. I will ensure that my child's device has parental controls installed as appropriate to their age;
3. I will ensure that my child and all others in the household are wearing suitable clothing;
4. I will ensure my child is accessing online learning from a suitable device and in an area of the home that I can monitor;
5. I will ensure that language used is appropriate, including any family members in the background.
6. I will support my child in logging on to their MS Teams Class with the full name displayed;
7. I will not contribute to the live lesson whilst it is in progress;
8. I understand that a live class will be recorded and kept for up to a year so that the video can be reviewed;
9. I will not video or screenshot or share the live lesson beyond MS Teams and understand that this is to safeguard mine and other children;
10. If I see or hear anything concerning, whilst my child is accessing learning online, I will immediately report it to school staff via the agreed communication channel.
11. I understand that teachers are available for remote learning during school hours and that they will provide feedback on submitted assignments within an agreed timeframe.

I have read and understand the above and agree to engage with remote learning within these guidelines.

Children/s Name/s:

Parent Name:

Signed:

Date:

Appendix 3

Application form to set up an official school/trust social media account

Location proposed account will relate to i.e. school name	
Department/area account will relate to if not whole school i.e. PE/Nursery	
Type/s of account i.e. Facebook/Twitter	
Proposed name of the account	
Name/s of individuals who will be responsible for implementing, maintaining, and monitoring account (two individuals as a minimum)	
Reason/s for the proposed account	
The intended audience for the account	
How the account will be promoted	
Will the account be open/private/closed?	
Date submitted:	
Permission is given to create an account Y/N	

Name of senior leader granting permission (Print & sign)	

Appendix 4

Procedure for 1:1 Sessions for Staff and Pupils

In accordance with DfE Guidance Safeguarding and Remote Education, schools should consider if 1:1 sessions are appropriate in some circumstances. Before scheduling a 1:1 session this should be discussed and approved by the Senior Leadership Team and included in the school Covid risk assessment, identifying relevant control measures.

The following protocols apply to a 1:1 session in a primary school:

- Parents and carers have been informed that 1:1 form part of the approaches that may be used by a teacher or support staff member;
- All sessions must be conducted on MS Teams;
- Sessions should take place in either a school space or a public area of your house;
- If you are delivering the session from your home, no one in your house should be able to hear the conversation;
- Sessions should be scheduled by the teacher or support staff;
- During the session, the pupil video will be switched on and sessions may be recorded. Where recording, sessions must be conducted in a private channel;
- All staff will adhere to requirements of safeguarding, acceptable use policy, and code of conduct;
- Any concerns will be responded to in line with the agreed safeguarding procedures;
- Recordings of sessions will be allowed to expire in 21 days unless a concern has been raised. In this case, the recording will be downloaded and saved.

The following protocols apply to a 1:1 session in the Secondary School:

- Permission is granted by a parent or legal guardian, a note of this must be recorded on the Go 4 Schools communication log
- Students should keep their cameras switched off
- Session should take place in either a school space 4or a public area of your house E.G not in the bedroom
- If you are delivering the session from your home it must be private and no one in your house should be able to hear the conversation
- A record of the session (not the details) to be recorded on the Go 4 Schools communication log
- If there are any safeguarding concerns raised during the session these need to be logged on CPOMS

Appendix 5

Individual pupil risk assessment for 1:1 remote meetings

The purpose of this risk assessment is to document the risk factors for the named student and what measures are in place to manage them so that a 1:1 meeting via Teams can take place as safely as possible. A copy of this MUST be stored on CPOMS along with the outcomes of the meeting.

Pupil name:	**Pupil year group:**	**Date:**
Areas of concern:		
What health and safety hazards could arise:		
What support has already been put in place:		
Which activities cannot be safely managed, as far as it is possible to foresee?		

Activity	**Risk Factor**	**Controls**	**Comments/actions**	**Risk factor after controls applied**	**A consequence of failure to meet this requirement**