# Prime8 Education

Online Safety Policy
Including Acceptable Use

## Development, Monitoring & Review of this Policy

This online safety policy has been developed by:

- Director
- Online Safety Coordinator
- Staff – including teachers, support staff, technical staff
- Parents and carers
- Community users

## Schedule for Development/Monitoring/Review

| | |
|---|---|
| The implementation of this online safety policy will be monitored by the: | Director and Senior Leadership Team |
| Monitoring will take place at regular intervals: | Termly |
| The online safety policy will be reviewed annually, or more regularly in the light of significant developments in the use of technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be: | August 2026 |
| Should serious online safety incidents take place, the following external persons/agencies should be informed: | NCC<br>Safeguarding Officer<br>Schools/Academies<br>LADO<br>Police |

Prime8 Education will monitor the impact of the policy using:

- Logs of reported incidents

## Scope of the Policy

This policy applies to all members of Prime8 Education (including staff, learners, volunteers, parents/carers, visitors, community users) who have access to and are users of Prime8's digital technology systems, both in and out of the Provision.

The Education and Inspections Act 2006 empowers leaders to such extent as is reasonable, to regulate the behaviour of learners when they are off Prime8 site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of online bullying or other online safety incidents covered by this policy, which may take place outside of Prime8, but is linked to membership of the Provision. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

Prime8 will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that take place out of the Provision.

## Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within Prime8 Education.

### Director and DSLs

The Director and DSLs are responsible for the approval of the online safety policy and for reviewing the effectiveness of the policy. This will be carried out by the Director and DSLs receiving regular information about online safety incidents and monitoring reports. The DSLs work with the IT Technical lead as the Online Safety Lead. The role of the Online Safety Lead will include:

- meetings with the Online Safety Co-ordinator
- regular monitoring of online safety incident logs
- reporting to relevant key personnel

### Senior Leaders

- Senior leaders have a duty of care for ensuring the safety (including online safety) of members of the Prime8 community, though the day-to-day responsibility for online safety will be delegated to the *Online Safety Lead*.
- The Senior Leadership Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. (See flow chart on dealing with online safety incidents – included in a later section
- The Senior Leaders are responsible for ensuring that the Online Safety Lead and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Senior Leadership Team will receive regular monitoring reports from the Online Safety Lead.

### Online Safety Lead

- leads the Online Safety Group
- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the online safety policies/documents

- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- provides training and advice for staff
- liaises with the Local Authority
- liaises with technical support
- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments
- attends relevant meetings with the Director
- reports regularly to Senior Leadership Team

## Technical Lead

Is responsible for ensuring:

- that Prime8's technical infrastructure is secure and is not open to misuse or malicious attack
- that Prime8 meets required online safety technical requirements and any Local Authority online safety policy/guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy
- that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- that the use of the networks/internet/digital technologies is regularly monitored in order that any misuse/attempted misuse can be reported to the Director and Senior Leaders; Online Safety Lead for investigation/action/sanction
- that monitoring software/systems are implemented and updated as agreed in Prime8 policies

## Teaching and Support Staff

Are responsible for ensuring that:

- they have an up-to-date awareness of online safety matters and of the current online safety policy and practices
- they have read, understood and signed the staff acceptable use policy/agreement (AUP/AUA)
- they report any suspected misuse or problem to the Director/Online Safety Lead for investigation/action/sanction
- all digital communications with learners/parents/carers should be on a professional level and only carried out using official Prime8 systems
- online safety issues are embedded in all aspects of the curriculum and other activities
- learners understand and follow the Online Safety Policy and acceptable use policies
- learners have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras, etc. in lessons (where allowed) and implement current policies with regard to these devices

- in lessons where internet use is pre-planned learners should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

## Designated Safeguarding Lead

The DSL should be trained in online safety issues and be aware of the potential for serious child protection/safeguarding issues to arise from:

- sharing of personal data
- access to illegal/inappropriate materials
- inappropriate on-line contact with adults/strangers
- potential or actual incidents of grooming
- online-bullying

## Online Safety Group

The Online Safety Group provides a consultative group that has wide representation from Prime8, with responsibility for issues regarding online safety and the monitoring the Online Safety Policy including the impact of initiatives.

Members of the Online Safety Group (or other relevant group) will assist the Online Safety Lead with:

- the production/review/monitoring of the online safety policy/documents.
- mapping and reviewing the online safety/digital literacy curricular provision – ensuring relevance, breadth and progression
- monitoring network/internet /incident logs
- consulting stakeholders – including parents/carers, commissioners and the learners about the online safety provision

## Learners:

- are responsible for using Prime8's digital technology systems in accordance with the learner acceptable use agreement
- will be taught research skills and the need to avoid plagiarism and uphold copyright regulations
- will be taught the importance of reporting abuse, misuse or access to inappropriate materials and know how to report issues and who to
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking/use of images and on online-bullying.
- should understand the importance of adopting good online safety practice when using digital technologies out of Provision and realise that Prime8's online safety policy covers their actions out Prime8, if related to their membership of the Provision.

## Parents/carers

Parents/carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. Prime8 will take every opportunity to help parents

understand these issues through newsletters, letters, website, and information about national/local online safety campaigns/literature. Parents and carers will be encouraged to support Prime8 in promoting good online safety practice and to follow guidelines on the appropriate use of:

- access to parents' sections of the website
- their children's personal devices in Prime8

# Policy Statements

## Education – Learners

Whilst regulation and technical solutions are very important, their use must be balanced by educating learners to take a responsible approach. The education of learners in online safety/digital literacy is therefore an essential part of Prime8's online safety provision. Children and young people need the help and support of the Provision to recognise and avoid online safety risks and build their resilience.

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned online safety curriculum should be provided as part of PHSE and should be regularly revisited
- Learners should be taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information.
- Learners should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Learners should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.
- Learners should be helped to understand the need for the learner acceptable use agreement and encouraged to adopt safe and responsible use both within and outside Prime8.
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices
- In lessons where internet use is pre-planned, it is best practice that learners should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where learners are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, learners may need to research topics (e.g., racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Lead can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

## Education – Parents/carers

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring/regulation of the children's online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

Prime8 will therefore seek to provide information and awareness to parents and carers through:

- Letters, newsletters, web site
- Reference to the relevant web sites/publications e.g. swgfl.org.uk, www.saferinternet.org.uk/, http://www.childnet.com/parents-and-carers

## Education & Training – Staff/Volunteers

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of online safety training will be made available to staff through EduCare. This will be regularly updated and reinforced. Courses include *Online Safety* and *Safer Blended Learning.*
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the online safety policy and acceptable use agreements.
- It is expected that some staff will identify online safety as a training need within the performance management process and will be directed to relevant courses.
- This online safety policy and its updates will be presented to and discussed by staff in staff meetings.
- The Online Safety Lead will provide advice/guidance/training to individuals as required.

## Technical – infrastructure/equipment, filtering and monitoring

Prime8 will be responsible for ensuring that the infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities:

- Technical systems will be managed in ways that ensure that Prime8 meets recommended technical requirements
- There will be regular reviews of the safety and security of Prime8's technical systems
- All users will have clearly defined access rights to the technical systems and devices.
- All users will be provided with a username and secure password by Alison Bryant (DSL) who will keep an up-to-date record of users and their usernames. Users are responsible for the security of their username and password.

- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband. Content lists are regularly updated, and internet use is logged and regularly monitored.
- Internet filtering/monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet.
- Technical staff can regularly monitor and record the activity of users on the technical systems and users are made aware of this in the acceptable use agreement.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, workstations, mobile devices, etc. from accidental or malicious attempts which might threaten the security of Prime8 systems and data. The infrastructure and individual devices are protected by up-to-date virus software.

## Mobile Technologies (including BYOD/BYOT)

Mobile technology devices may be owned or provided by Prime8, the LA (Local Authority) or personally owned and might include smartphone, tablet, notebook/laptop or other technology that usually has the capability of utilising the Prime8's wireless network. The device then has access to the wider internet which may include cloud-based services such as email and data storage.

All users should understand that the primary purpose of the use of mobile or personal devices at Prime8 is educational. The mobile technologies policy should be consistent with and inter-related to other relevant polices including but not limited to the safeguarding policy, behaviour policy, bullying policy, acceptable use policy, and policies around theft or malicious damage. Teaching about the safe and appropriate use of mobile technologies is an integral part of Prime8's online safety education programme.

- The acceptable use agreements for staff, learners and parents/carers will give consideration to the use of mobile technologies

- Prime8 Education allows:

| | Provision Devices | | | Personal Devices | | |
|---|---|---|---|---|---|---|
| | Prime8 owned for single user | Prime8 owned for multiple users | Authorised device[1] | Learner owned | Staff owned | Visitor owned |
| Allowed in provision | Yes | Yes | Yes | Yes | Yes | Yes |
| Full network access | Yes | Yes | Yes | No | Yes | No |

Aspects that Prime8 have considered include:

Provision owned/provided devices:

- Who they will be allocated to?
- Where, when and how their use is allowed – times/places/in provision/out of provision
- If personal use is allowed
- Levels of access to networks/internet (as above)
- Management of devices/installation of apps/changing of settings/monitoring
- Network/broadband capacity
- Technical support
- Filtering of devices
- Access to cloud services
- Data Protection
- Taking/storage/use of images
- Exit processes – what happens to devices/software/apps/stored data if user leaves Prime8
- Liability for damage
- Staff training

Personal devices:

- Which users are allowed to use personal mobile devices in provision?
- Restrictions on where, when and how they may be used in provision
- Storage
- Whether staff will be allowed to use personal devices for Prime8 business
- Levels of access to networks/internet (as above)
- Network/broadband capacity
- Technical support (this may be a clear statement that no technical support is available)
- Filtering of the internet connection to these devices
- Data Protection
- The right to take, examine and search users' devices in the case of misuse
- Taking/storage/use of images
- Liability for loss/damage or malfunction following access to the network (likely to be a disclaimer about Prime8 responsibility).
- Identification/labelling of personal devices
- How visitors will be informed about Prime8 requirements
- How education about the safe and responsible use of mobile devices is included in the Prime8 online safety education programmes.

## Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and learners instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and learners need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for online bullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. Prime8 will inform and

educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate learners about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g., on social networking sites.
- Written permission from parents or carers will be obtained before photographs of learners are published on the website, on social media or in the local press
- Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow Prime8 policies concerning the sharing, distribution and publication of those images. Those images should only be taken on Prime8 equipment; the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital/video images that learners are appropriately dressed and are not participating in activities that might bring the individuals or Prime8 into disrepute.
- Learners must not take, use, share, publish or distribute images or videos of others without permission from staff as well as the subject
- Photographs published on the website, or elsewhere that include learners will be selected carefully and will comply with good practice guidance on the use of such images.
- Learners' full names will not be used anywhere on the website, particularly in association with photographs.
- Learner's work, which identifies the learner, can only be published with the permission of the learner and parents or carers.

Learners and parents/carers will also complete a phone expectations agreement on joining and Learners will re-sign this agreement at the beginning of each academic year.

## Data Protection

Personal data will be recorded, processed, transferred and made available according to the current data protection legislation.

Prime8 must ensure that:

- it has a Data Protection Policy.
- it implements the data protection principles and is able to demonstrate that it does so through use of policies, notices and records.
- it will hold only the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for. Prime8 should develop and implement a 'retention policy" to ensure there are clear and understood policies and routines for the deletion and disposal of data to support this. personal data held must be accurate and up to date where this is necessary for the purpose it is processed for. Have systems in place to identify inaccuracies, such as asking parents to check emergency contact details at suitable intervals
- it provides staff, parents, volunteers, and learners with information about how Prime8 looks after their data

- IT system security is ensured and regularly checked. Patches and other security essential updates must be applied promptly to protect the personal data on the systems. Administrative systems are securely ring fenced from systems accessible in the classroom/to learners
- it has undertaken appropriate due diligence and has required data processing clauses in contracts in place with any data processors where personal data is processed.
- it understands how to share data lawfully and safely with other relevant data controllers.
- it reports any relevant breaches to the Information Commissioner within 72hrs of becoming aware of the breach in accordance with UK data protection law. It also reports relevant breaches to the individuals affected as required by law.
- all staff receive data protection training at induction and appropriate refresher training thereafter. Staff undertaking particular data protection functions, such as handling requests under the individual's rights, will receive training appropriate for their function as well as the core training provided to all staff.

When personal data is stored on any mobile device or removable media the:

- data must be encrypted, and password protected.
- device must be password protected.
- device should be protected by up-to-date virus and malware checking software.

Staff must ensure that they:

- take care to ensure the safe keeping of personal data at all times, minimising the risk of its loss or misuse
- can recognise a possible breach, understand the need for urgency and know who to report it to within Prime8
- can help data subjects understand their rights and know how to handle a request whether verbal or written
- know that where personal data is stored or transferred on mobile or other devices (including USBs), these must be encrypted, and password protected.
- will not transfer any Prime8 personal data to personal devices except as in line with Provision policy
- access personal data sources and records only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data

# Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the provision currently considers the benefit of using these technologies for education outweighs their risks/disadvantages:

| Communication Technologies | Staff and Other Adults | | | | Learners | | | |
|---|---|---|---|---|---|---|---|---|
| | Allowed | Allowed at certain times | Allowed for selected staff or with Director permission | Not Allowed | Allowed | Allowed at certain times | Allowed with staff permission | Not Allowed |
| Mobile phones may be brought to Prime8 | Y | | | | Y | | | |
| Use of mobile phones in lessons | | Y | | | | | | Y |
| Use of mobile phones in social time | Y | | | | | Y | | |
| Taking photos on mobile phones or cameras | | Y | | | | | | Y |
| Use of other mobile devices, e.g., tablets or gaming devices | | Y | | | | Y | | |
| Use of personal email address when at Prime8 or on the Prime8 Network | | Y | | | | | | Y |
| Use of Prime8 email for personal emails | | | | Y | | | | Y |
| Use of messaging apps | Y | | | | | Y | | |
| Use of social media | | | | Y | | Y | | |
| Use of Blogs | | | | Y | | | | Y |

When using communication technologies, Prime8 considers the following as good practice:

- The official email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and learners should therefore use only Prime8 email service to communicate with others when in provision, or on Prime8 systems (e.g., by remote access).

- Users must immediately report to the nominated person – in accordance with Prime8 policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and learners or parents/carers (email, social media, chat, blogs, etc) must be professional in tone and content. These communications may only take place on official (monitored) systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Learners at KS2 and above will be provided with individual Prime8 email addresses for educational use as and when required
- Learners will be taught about online safety issues, such as the risks attached to the sharing of personal details. They will also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information will not be posted on the Prime8 website and only official email addresses should be used to identify members of staff.

## Social Media - Protecting Professional Identity

All schools, academies, MATs and local authorities have a duty of care to provide a safe learning environment for learners and staff. Schools/academies, MATs and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, engage in online bullying, discriminate on the grounds of sex, race or disability or who defame a third party may render the Provision or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

Prime8 provides the following measures to ensure reasonable steps are in place to minimise risk of harm to learners, staff and the provision through:

- Ensuring that personal information is not published
- Training is provided including: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

Prime8 staff should ensure that:

- No reference should be made in social media to learners, parents/carers or Prime8 staff
- They do not engage in online discussion on personal matters relating to members of Prime8 community
- Personal opinions should not be attributed to the Provision or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information

Personal Use:

- Personal communications are those made via a personal social media account. In all cases, where a personal account is used which associates itself with the Provision or impacts on it, it must be made clear that the member of staff is not communicating on behalf of Prime8 with an appropriate disclaimer. Such personal communications are within the scope of this policy
- Personal communications which do not refer to or impact upon Prime8 are outside the scope of this policy
- Where excessive personal use of social media in Provision is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
- Prime8 permits reasonable and appropriate access to private social media sites

Monitoring of Public social media:

- As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about Prime8
- Prime8 should effectively respond to social media comments made by others according to a defined policy or process (please refer to the Director)

# Dealing with unsuitable/inappropriate activities

Some internet activities e.g., accessing child abuse images or distributing racist material is illegal and would obviously be banned from Prime8 and all other technical systems. Other activities e.g., cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a Provision context, either because of the age of the users or the nature of those activities.

Prime8 believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in/or outside Prime8 when using equipment or systems. This policy restricts usage as follows:

| User Actions | Acceptable | Acceptable at certain times | Acceptable for nominated users | Unacceptable | Unacceptable and illegal |
|---|---|---|---|---|---|

| | | | | | | |
|---|---|---|---|---|---|---|
| Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to: | Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978 | | | | | X |
| | Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003. | | | | | X |
| | Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008 | | | | | X |
| | Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986 | | | | | X |
| | Pornography | | | | | X |
| | Promotion of any kind of discrimination | | | | | X |
| | Threatening behaviour, including promotion of physical violence or mental harm | | | | | X |
| | Promotion of extremism or terrorism | | | | | X |
| | Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the Prime8 or brings the provision into disrepute | | | | | X |

| | | | | | |
|---|---|---|---|---|---|
| Activities that might be classed as cyber-crime under the Computer Misuse Act:<br>• Gaining unauthorised access to Prime8 networks, data and files, through the use of computers/devices<br>• Creating or propagating computer viruses or other harmful files<br>• Revealing or publicising confidential or proprietary information (e.g., financial / personal information, databases, computer / network access codes and passwords)<br>• Disable/Impair/Disrupt network functionality through the use of computers/devices | | | | | X |
| • Using penetration testing equipment (without relevant permission) | | | | | X |
| Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the Provision | | | | X | |
| Revealing or publicising confidential or proprietary information (e.g., financial/personal information, databases, computer/network access codes and passwords) | | | | X | |
| Unfair usage (downloading/uploading large files that hinders others in their use of the internet) | | | | X | |
| Using Prime8 systems to run a private business | | | | X | |
| Infringing copyright | | | | X | |
| On-line gaming (educational) | | | X | | |
| On-line gaming (non-educational) | | | X | | |
| On-line gambling | | | | | X |
| On-line shopping/commerce | | | | X | |
| File sharing | | | X | | |
| Use of social media | | | X | | |

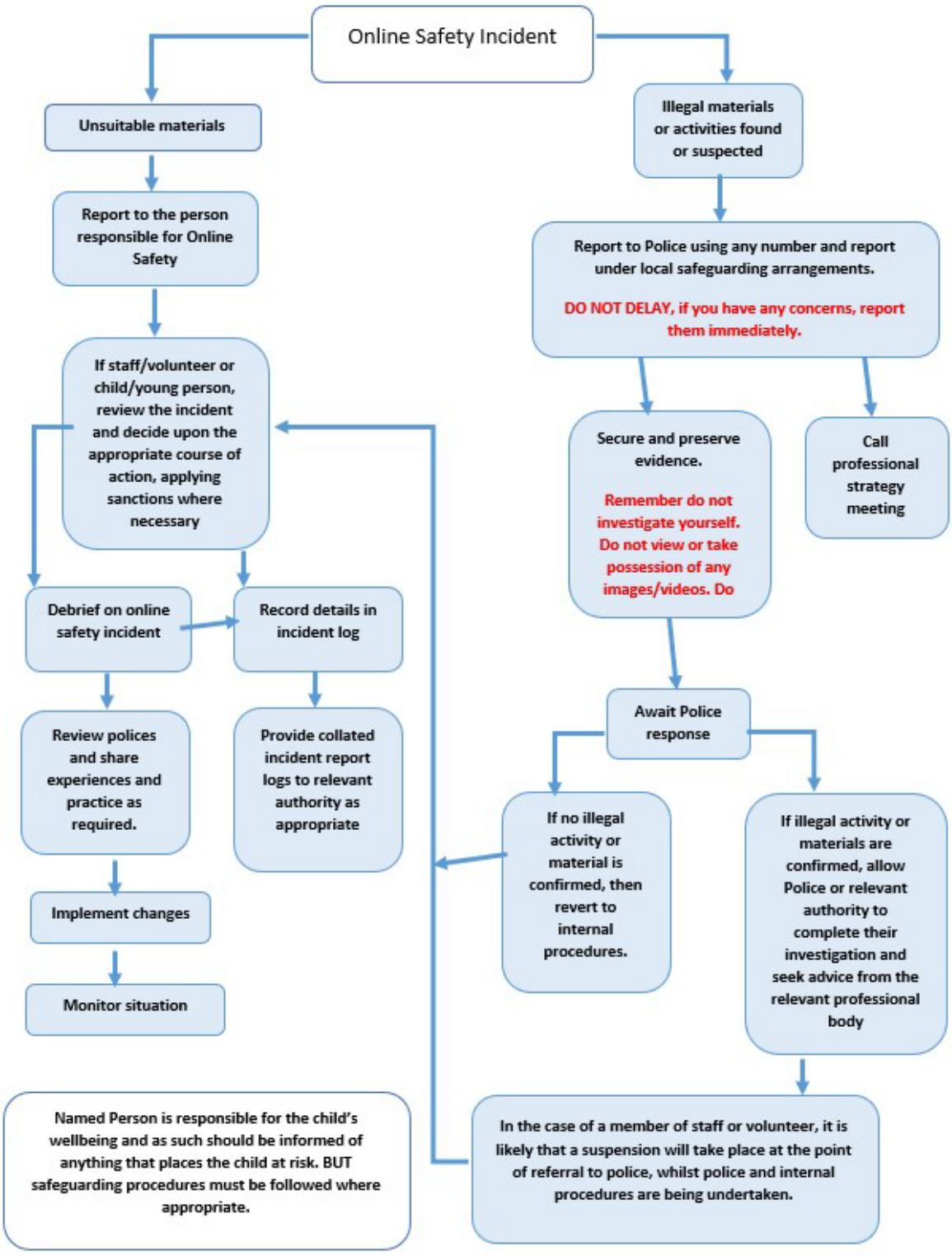
| | | | | | |
|---|---|---|---|---|---|
| Use of messaging apps | | | X | | |
| Use of video broadcasting e.g., YouTube | | | X | | |

# Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see “User Actions” above).

# Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right-hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police as well as the Director and DSL.




# Other Incidents

It is hoped that all members of Prime8 community will be responsible users of digital technologies, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary, can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
    - Internal response or discipline procedures
    - Involvement by Local Authority.
    - Police involvement and/or action
- If content being reviewed includes images of child abuse, then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:
    - incidents of 'grooming' behaviour
    - the sending of obscene materials to a child
    - adult material which potentially breaches the Obscene Publications Act
    - criminally racist material o promotion of terrorism or extremism
    - offences under the Computer Misuse Act (see User Actions chart above)
    - other criminal conduct, activity or materials
- Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for the Provision and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

# Provision actions & sanctions

It is more likely that Prime8 will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures as follows:

| Learner Incidents | Actions/Sanctions | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | Refer to class teacher/tutor | Refer to DSL | Refer to Director | Refer to Police | Refer to technical support staff for action re filtering/security etc. | Inform parents/carers | Removal of network/internet access rights | Warning | | |
| Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/inappropriate activities). | | X | X | X | | | | | | |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Unauthorised use of non-educational sites during lessons | X | | | | | | | | |
| Unauthorised/inappropriate use of mobile phone/digital camera/another mobile device | X | X | | | | | | | |
| Unauthorised/inappropriate use of social media/ messaging apps/personal email | X | X | | | | | | | |
| Unauthorised downloading or uploading of files | | X | X | | | | | | |
| Allowing others to access provision network by sharing username and passwords | | X | X | | | | | | |
| Attempting to access or accessing the provision network, using another learner's account | X | X | | | X | X | | | |
| Attempting to access or accessing the provision network, using the account of a member of staff | | X | X | | X | X | | | |
| Corrupting or destroying the data of other users | | X | X | | | | | | |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature | | | X | | | X | | | |
| Continued infringements of the above, following previous warnings or sanctions | | | X | | | X | X | | |
| Actions which could bring Prime8 into disrepute or breach the integrity of the ethos of the provision | | | X | | | X | X | | |
| Accidentally accessing offensive or pornographic material and failing to report the incident | | | X | | X | X | X | | |
| Deliberately accessing or trying to access offensive or pornographic material | | | X | | X | X | X | | |
| Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act | | | X | | X | X | X | | |

Actions/Sanctions

| Staff Incidents | Refer to line manager | Refer to Headteacher | Refer to Local Authority/HR | Refer to Police | Refer to Technical Support Staff for action re filtering | Warning | Suspension | Disciplinary action |
|---|---|---|---|---|---|---|---|---|
| Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/inappropriate activities). | | X | X | X | | | | |
| Inappropriate personal use of the internet/social media/personal email | X | X | | | | | | |
| Unauthorised downloading or uploading of files | X | | | | | | | |
| Allowing others to access provision network by sharing username and passwords or attempting to access or accessing the provision network, using another person's account | | X | | | X | X | | |
| Careless use of personal data e.g., holding or transferring data in an insecure manner | X | | | | | | | |
| Deliberate actions to breach data protection or network security rules | | X | | | X | | | X |
| Corrupting or destroying the data of other users or causing deliberate damage to hardware or software | | X | | | | | | X |
| Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature | X | X | | | | X | | |
| Using personal email/social networking/instant messaging/text messaging to carrying out digital communications with learners | X | X | | | | X | | |
| Actions which could compromise the staff member's professional standing | X | X | | | | | | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Actions which could bring the Provision into disrepute or breach the integrity of the ethos of it | | X | | | | X | | |
| Accidentally accessing offensive or pornographic material and failing to report the incident | | X | | | | X | | |
| Deliberately accessing or trying to access offensive or pornographic material | | X | | | | | | X |
| Continued infringements of the above, following previous warnings or sanctions | | X | | | | | | X |

## Acceptable Use Policy – Updated 2023 – see *Appendix 1*

## Further Information:

1. Microsoft TEAMS has been assessed and approved by Julie Townsend Director and Iain Balmer ICT consultant.
2. Staff will only use Prime8 Education managed accounts with learners and parents/carers. Use of any personal accounts to communicate with learners and/or parents/carers is not permitted. Any pre-existing relationships or situations which mean this cannot be complied with will be discussed with DSL or director.
   Staff will use work provided equipment where possible e.g., a setting laptop, tablet or other mobile device.
3. All remote lessons will be formally timetabled; Director, Provision Manager or DSL is able to drop in at any time.
4. Live streamed remote learning sessions will only be held with approval and agreement from the Director or Provision Manager.

**Data Protection and Security**

5. Any personal data used by staff and captured by Microsoft TEAMS when delivering remote learning will be processed and stored with appropriate consent and in accordance with our data protection policy.
6. All remote learning and any other online communication will take place in line with current Prime8 Education confidentiality expectations.
7. Staff will not record lessons or meetings using personal equipment unless agreed and risk assessed by SLT and in line with our data protection policy requirements.
8. Access to Microsoft TEAMS will be managed in line with current IT security expectations as outlined in the online safety policy.

**Session Management**

9. Appropriate privacy and safety settings will be used to manage access and interactions. This includes: disabling/limiting chat, staff not permitting learners to share screens, keeping meeting IDs private
10. Live 1 to 1 sessions will only take place with approval from the Director. A parent/carer should be present in the room if possible (however, this may not be appropriate if providing counselling or safeguarding support). These should be recorded where there is a potential safeguarding concern.
11. Alternative approaches and access for Remote Learning will be provided to those who do not have access.

**Behaviour Expectations**

12. Staff will model safe practice and moderate behaviour online
13. Staff will remind learners of behaviour expectations and reporting mechanisms at the start of the session.
14. When sharing videos and/or live streaming, participants are required to:
    - wear appropriate dress.
    - ensure backgrounds of videos are neutral (blurred if possible).
    - ensure that personal information and/or unsuitable personal items are not visible, either on screen or in video backgrounds.
15. Educational resources will be used or shared in line with our existing teaching and learning policies, taking licensing and copyright into account.

**Policy Breaches and Reporting Concerns**

16. Participants are encouraged to report concerns during remote and live streamed sessions:
17. Inappropriate online behaviour will be responded to in line with existing policies such as acceptable use of technology, allegations against staff, anti-bullying and behaviour.
18. Sanctions for deliberate misuse may include:
    - restricting/removing use, contacting police if a criminal offence has been committed

| | | |
|---|---|---|
| Date of Completion | 1.9.25 | Signed: Debbie Crookes (Tutor) |
| Date of Ratification | 1.9.2025 | Signed: Julie Townsend (Director) |
| Date for Review | August 2026 | |

# Acceptable Use Policy for Use of Computers and Online Communication

## Parents/Carers and Learners

Prime8 Education has provided computers for use by learners as an important tool for learning. Use of Prime8 devices by learners, is governed at all times by the following policy.
There may also be the need for remote learning again at some point, and the Prime8 Acceptable Use Policy covers Remote Learning as well as using Computers during sessions.
Please read the following Acceptable Use Policy and sign to show agreement on behalf of you and your child.

**All learners have a responsibility to use the computer system in an educational, lawful, and ethical manner.**
**Deliberate abuse of the computer system will lead to consequences being put in place. Please note that this is to safeguard all users.**

- You should not share your password or logon details with others.
- Access links should not be made public, forwarded or shared by yourself or parents/carers without prior staff permission
- You must not allow another learner to have individual use of your account under any circumstances, for any length of time, even if supervised
- You must not connect personal computer equipment to the computer equipment without prior approval from staff
- You must at all times conduct your computer usage appropriately, which includes being polite and using the system in a safe, legal and education appropriate manner
- Among uses that are considered unacceptable are the following: inappropriate, offensive, pornographic, abusive, threatening, racist, or sexist, language or materials; making ethnic, sexual-preference, or gender-related slurs or jokes
- You must respect, and not attempt to bypass, security or access restrictions in place on the computer system
- You must not intentionally damage, vandalise, disable, or otherwise harm the operation of computers
- You must not download material from the Internet, or print without staff permission
- You must not eat or drink around computer equipment
- Staff may monitor sessions to ensure compliance with this Acceptable Use Policy and applicable laws including copyright laws
- You must not store sensitive personal information on the computer system that is unrelated to Prime8 activities (such as personal passwords, photographs, or music)

- You should report any problems that need attention to a member of staff as soon as possible
- If you suspect your computer has been affected by a virus or other malware, you must report this to a member of staff immediately
- If you have lost documents or files, you should report this to a member of staff as soon as possible
- All learners have a duty to ensure this Acceptable Use Policy is followed
- You must immediately inform a member of staff, of abuse of any part of the computer system.
- In particular, you should report:
  - any websites accessible that you feel are unsuitable;
  - any inappropriate content suspected to be stored on the computer;
  - any breaches, or attempted breaches, of computer security
- Learners are responsible for performing routine maintenance which may include:
  - removing old and unused files/folders/shortcuts;
  - not downloading or creating large files;
  - emptying the recycle bin periodically
- Any Remote learning will only take place using Microsoft TEAMS.
- Remote Learning Sessions must not be recorded, and screenshots or photographs should not be taken and/or shared.
- Remote Learning should be attended in a shared/communal space or room with an open door, appropriately supervised by a parent/carer or another appropriate adult.
- Sanctions for deliberate misuse may include restricting/removing use or contacting police if a criminal offence has been committed.

Use of the Prime8 computer system also indicates your consent to the Acceptable Use Policy and monitoring taking place.

*I have read and understood Prime8 Education's Acceptable Use Policy for Remote Learning and Online Communication.*

Learner Signature: _____ Learner Name: _____

Parent/Carer Signature: _____ Parent/Carer Name: _____

Date: _____