ICT Misuse Policy

Aim

The ICT (Information and Communication Technology) Misuse Policy aims to ensure any allegation, which is to be made in respect of the intentional or unintentional misuse of any online technologies, is to be addressed to in a responsible and calm manner. This includes any known or suspected breaches of the Acceptable Use Policy, Confidentiality policy and E-safety policy.

- Allegations will be dealt with promptly, sensitively and fairly in line with agreed procedures. The ICT Misuse Policy outlines the sanctions that are to be applied should an incident occur.
- The overall priority is to ensure the safety and wellbeing of children and young people at all times. Should it be suspected at any stage that a child or young person may have been or is considered to be subject to abuse, the Safeguarding & Child Protection Policy and Procedures will be implemented with immediate effect. These procedures will also be followed should an allegation of abuse be made against any employee, manager, volunteer or student. The Safeguarding & Child Protection Policy takes precedence over all others, and referrals must be made to the appropriate agency as deemed necessary.

Scope

The ICT Misuse Policy applies to all individuals who are to have access to and/or be users of work-related ICT systems. This includes children and young people, parents and carers, early years practitioners and their managers, volunteers, students, visitors and contractors. This list is not to be considered exhaustive.

- The policy is implemented in respect of any potential breaches of the Acceptable Use Policy, Confidentiality Policy, & E-Safety Policy.

Responsibilities

The registered person and the Safeguarding Designated Officer is responsible for ensuring that the procedures outlined herein will be followed. These procedures are considered should an allegation of misuse be made against a child, young person or adult.

Policy statement

It will be ensured that:

- Relevant online safety policies and procedures are fully implemented, monitored and reviewed. The Designated Lead for Safeguarding is responsible for the management of such policies.
- All ICT users are aware of possible signs of potential misuse. Adults, in particular, are responsible for observing practice and behaviours, so that any significant changes in such are identified at the earliest opportunity.
- All ICT users are aware that the misuse of ICT and/or breaches of relevant policies and, procedures are to be taken seriously. All ICT users are aware of the potential sanctions that could be applied should such concerns be raised.
- Effective reporting and whistle-blowing procedures are in place and promoted.
- It is to be acknowledged, however, that no system or procedure can be considered 100 per cent safe, secure and fool-proof. It should therefore be accepted that the

potential for ICT to be misused, whether intentionally or unintentionally remains. The aim of the online safety policies will therefore be to minimise such opportunities and risk.

Procedures

- All incidents will be dealt with on an individual case by case basis, and an escalating tariff of agreed sanctions will be put in place.
- The context, intention and impact of each incident will determine the response and actions to be taken. This will allow for a degree of flexibility as to how sanctions are to be applied, subject to the need for other policies to be implemented. For example, a series of minor incidents by one individual is likely to be treated differently than should it be deemed a one-off occurrence; similarly, unintentional and intentional access to inappropriate websites will instigate different levels of intervention and sanctions.
- All online safety incidents will be recorded and monitored, and any potential patterns in behaviours should be identified, to enable such issues to be addressed proactively and for protection to be afforded.
- Misuse is to be categorised under the three headings of 'minor incidents', 'significant incidents' and 'serious incidents'.

Minor incidents

The following procedure is to be followed should an incident be considered minor.

- The incident will be reported to the Designated Safeguarding Lead. A written incident record will be made, and the situation monitored.
- The context, intention and impact of such misuse will also be considered. Where deemed necessary the incident will be escalated to a 'significant' or 'serious' level.
- Sanctions will be applied in accordance with the Acceptable Use Policy.

Significant incidents

There will always be the possibility that through access to the internet children and young people may gain unintentional access to inappropriate materials. Such material may not be illegal, but is not to be considered suitable in a childcare environment and/or to be age appropriate.

An open reporting policy is in place which means that all inadvertent breaches and access to inappropriate materials must be reported. The non-reporting of such breaches will result in the concern being escalated.

The following procedure will be followed should an incident be considered significant.

- The incident will be reported to the DSL. A written incident record will be made.
- The context, intention and impact of such misuse will be considered. Where deemed necessary the incident will be escalated to a 'serious' level.
- Appropriate action will be taken by the DSL.
- If the incident should relate to the inadvertent access to an inappropriate website, will be added to the banned or restricted list and filters will be applied, where relevant.
- Sanctions will be applied in accordance with the Acceptable Use Policy.

- In respect to misuse by children and young people, parents and carers will be informed of the alleged incident and advised of any actions to be taken as a result.

Serious incidents

- It must be ensured that all serious incidents will be dealt with promptly and reported to the DSL immediately.
- The context, intention and impact of the alleged misuse will be considered.
- Appropriate action will be taken by the DSL. All details will be accurately and legibly recorded. The reason why any decision is made will be also be noted.
- Should it be considered at any stage that a child or young person is or has been subject to abuse of any form, the Safeguarding & Child Protection Policy will be implemented with immediate effect. A referral will be made to Children's Services and the Police, where applicable.
- Should the incident relate to an allegation made against an employee, manager, volunteer or student; and there is a suggestion that a child or young person has been subjected to any form of abuse, the Safeguarding & Child Protection Policy will again be implemented with immediate effect. The Local Authority Designated Officer (LADO) must be contacted in the first instance in respect of any allegation made against an adult. The Police and Ofsted must also be contacted.
- It will be ensured that no internal investigation or interviews are to be carried out in respect of any allegations, unless it is to be explicitly requested otherwise by an investigating agency.
- It will be fully recognised that should allegations of abuse be made, children's Social Services, the Police and/or the Local Authority Designated Officer will be the investigative bodies. It must therefore be ensured that no action will be taken which could compromise any such investigations.
- Where applicable, any hardware implicated in any potential investigations of misuse will be secured, so that evidence can be preserved. This may include mobile phones, laptops, computers and portable media technology.
- Internal disciplinary procedures will not be undertaken until investigations by the relevant agencies are to have been completed. Legal or human resources advice will be sought prior to carrying out any internal investigations and/or instigating high level disciplinary procedures.
- On completion of both internal and external investigations, or sooner where it is deemed appropriate, an online safety review will be undertaken and policies and procedures will be amended and updated as necessary. A consultation on any proposed revisions will be held with all ICT users as appropriate. Revised policies and procedures will be circulated as applicable.
- By nature, serious incidents will most often involve illegal materials and activities, including the viewing, possession, taking, making and distribution of indecent images; bullying or harassment through the use of portable media devices, such as mobile phones or grooming. In such situations, these incidents may be instigated by a child, young person or adult.

The following incidents must always be reported to the Police, Children's Social Care, Local Authority Designated Officer and Ofsted:

- Discovery of indecent images of children and young people.
- Behaviour considered to be 'grooming'.
- Sending of obscene materials.

It should be understood, that by not reporting such incidents, an offence may be committed.

- The seriousness of such allegations are fully recognised, and it must be ensured that all such incidents are to be reported to the Police immediately. No attempt will be made to download, print or send any materials found. It is understood that further offences could be committed by doing so.
- Should potentially illegal material be discovered, as far as is reasonably practical, the equipment or materials found will not be touched. Computers or other devices will not be switched off unless it is authorised to do so by the Police. The focus must be on preventing further access to the illegal content by keeping other individuals out of the immediate area. Where necessary the monitor should be turned off (but the computer remains on).
- Illegal material and activities which must be reported to the Internet Watch Foundation.
- A report will be made to the Internet Watch Foundation www.iwf.org.uk/reporting.htm) should potentially illegal material, including images of child abuse be discovered. If it is unclear whether the content is to be considered illegal or not, the concern will be reported as a matter of caution.
- Should it be considered that materials are inappropriate but legal, such incidents will generally be dealt with through internal disciplinary procedures. Unless alleged criminal activity and/abuse is suspected, it will not normally be considered necessary to involve the Police or other agencies.

Media attention

- It is recognised that should a serious incident occur, it will most likely attract intense media interest and speculation. On such occasions, every possible attempt will be made to ensure that children and young people, parents and carers are protected from such influences.
- An agreed media strategy will be implemented, and statements will be released by authorised personnel, in accordance with information sharing procedures. In all instances, the prime concern will be the safeguarding and welfare of the children, young people and their families. Advice will be taken from Children's Services where appropriate before any media engagement is to be undertaken.

Authorisation & Review

This policy was adopted at a meeting of	Wroughton Preschool
Held on	
Date to be reviewed	Yearly at AGM
Signed on behalf of the management committee	
Name of signatory	
Role of signatory (e.g. chair/owner)	Chairperson