North Wolds Federation

ICT Acceptable Use Policy -Staff

October 2016

This policy is designed to safeguard both pupils and staff in school. All members of staff at the North Wolds Federation with access to the computer systems must sign to show they will adhere to this policy.

As of September 2016 the E Safety Office is Andrew Smith. The Safeguarding Governor is Marcus Hyde.

This policy should be considered alongside:

- **E Safety policy**
- **ICT Acceptable Use Policy- Children**
- **Safeguarding Policy**
- **Anti-Bullying Policy**
- **Twitter Policy**
- **Disciplinary Policy**
- **Whistleblowing Policy**

Monitoring of the School Network:
You should be aware that the school uses a facility called Securus to monitor internet traffic and records screen shots of pages that may be harmful or illegal. This is monitored on a weekly basis and records are kept of any issues raised. Search history and e-mail history can also be seen by senior staff.

Use of the World Wide Web:
You must not access or attempt to access any sites that contain any of the following:
child abuse

- pornography
- promoting discrimination of any kind
- promoting racial or religious hatred
- promoting illegal acts
- promoting extremism
- any other information which may be illegal or offensive to colleagues

It is recognised that under certain circumstances inadvertent access may happen. For example, a school researching the holocaust may produce results with Nazi propaganda. Should you or a student access any of these sites unintentionally you should report the matter to the e-safety officer so that it can be logged as a breach.

Access to any of the following should be reported to Lincolnshire Police:

- *images of child abuse (sometimes incorrectly referred to as child pornography). These are images of children apparently under 16 years old involved in sexual activity or posed to be sexually provocative; adult material that potentially breaches the Obscene Publications Act; criminally racist material in the UK.*

See Appendix One for Inappropriate Activity Flowchart

Social Networking:
Social networking is not permitted on school computers or laptops whilst in or out of the building unless the school Twitter Account is being accessed under the terms of the Twitter policy. If using Social Networking at home, Members of staff should never knowingly become “friends” with students on any social networking site or engage with pupils on internet chat. Members of staff using Social Networking should not disclose their place of work, place

any images taken on the school site or make any references to children, events in the school day, school polices or procedures. Disciplinary action may be taken against school staff who use social networking sites to publish anything that may be considered derogatory to the school. Staff using social networking are urged to ensure their privacy settings are high.

Use of Email - All members of staff should use their professional email address for conducting school business. Use of school email for personal use is not permitted.

Passwords - Staff should keep passwords private. Network passwords are confidential and individualised to each person. On no account should a member of staff allow a student to use a staff login.

Data Protection - Where a member of staff has to take home sensitive or confidential information sufficient safeguards should be in place to prevent loss or misuse. Members of staff will be issued with an encrypted memory stick for safe transfer of sensitive information. This includes tracking sheets, pupil details such as names or dates of birth and other records pertaining to children in school.

File sharing - technology such as peer to peer (P2P) and bit torrents is not permitted on the school network.

Personal Use - Staff are not permitted to use ICT equipment for personal use.

Images and Videos - Staff and pupils should not upload onto any internet site images or videos of themselves or other staff or pupils without consent of the e-safety officer.

Use of Personal ICT – Personal ICT may not be used in school due to the likelihood of it not being P.A.T tested and the risk of viruses being transferred to the school network.

Viruses and other malware - any virus outbreaks are to be reported to the Headteacher who will inform the PCSC UK helpdesk as soon as it is practical to do so, along with the name of the virus (if known) and actions taken by the school.

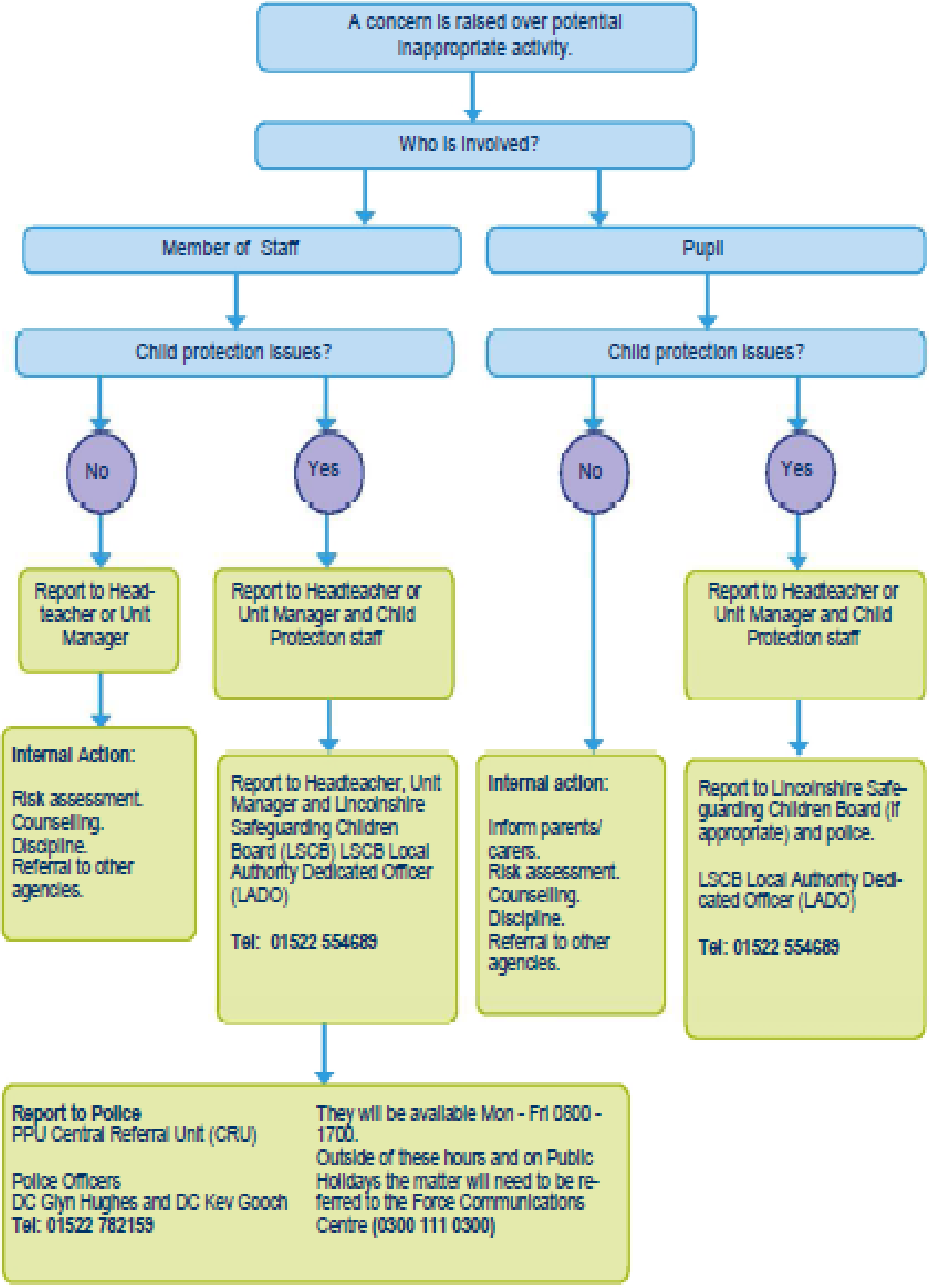
Loss of IT Equipment- Any loss of school IT equipment must be reported to the schools E safety office as soon after the loss as possible. This includes ipads, digital cameras, memory sticks and laptops. As a rule, IT equipment should be transported in a locked boot of a car for insurance reasons. IT equipment should not be left unattended in vehicles overnight.

Useful websites:
www.ceop.gov.uk
CEOP is a part of the UK police force dedicated to the eradication of child sexual abuse. There is an excellent educational programme, as well as advice and videos for all ages on their website.
www.iwf.org.uk
IWF (Internet Watch Foundation) provides the UK hotline to report criminal online content.
www.bbc.co.uk/cbbc/help/web/staysafe
BBC - a fantastic resource of e-safety information for the younger child.
Cybermentors is all about young people helping and supporting people online.
www.cybermentors.org.uk
Digital citizenship is about building safe spaces and communities, understanding how to manage personal information, and about being internet savvy - using your online presence to grow and shape your world in a safe, creative way, and inspiring others to do the same.
www.digizen.org

Signed Head teacher ____________________ Date _________

Signed Chair of Governors ____________________ Date _________

Inappropriate Activity flowchart



A concern is raised over potential inappropriate activity.

Who is involved?

Member of Staff

Child protection issues?

No

Report to Headteacher or Unit Manager

Internal Action:

Risk assessment.
Counselling.
Discipline.
Referral to other agencies.

Yes

Report to Headteacher or Unit Manager and Child Protection staff

Report to Headteacher, Unit Manager and Lincolnshire Safeguarding Children Board (LSCB) LSCB Local Authority Dedicated Officer (LADO)

Tel: 01522 554689

Report to Police
PPU Central Referral Unit (CRU)

Police Officers
DC Glyn Hughes and DC Kev Gooch
Tel: 01522 782159

They will be available Mon - Fri 0800 - 1700.
Outside of these hours and on Public Holidays the matter will need to be referred to the Force Communications Centre (0300 111 0300)

Pupil

Child protection issues?

No

Internal action:

Inform parents/ carers.
Risk assessment.
Counselling.
Discipline.
Referral to other agencies.

Yes

Report to Headteacher or Unit Manager and Child Protection staff

Report to Lincolnshire Safeguarding Children Board (if appropriate) and police.

LSCB Local Authority Dedicated Officer (LADO)

Tel: 01522 554689