CANLLAWIAU I YSGOLION A CHYMDEITHASAU RHIENI AC ATHRAWON

Diogelu Data (GDPR y DU) a Chydymffurfio â SDD DCT

1. Diben y Canllawiau Hyn

Datblygwyd y ddogfen hon i roi eglurhad a chyngor ymarferol i ysgolion, llywodraethwyr a Chymdeithasau Rhieni ac Athrawon (CRhAau) ynghylch eu cyfrifoldebau priodol wrth drin data personol a derbyn taliadau trwy gerdyn talu.

Er bod CRhAau yn sefydliadau elusennol annibynnol yn gyffredinol, yn aml mae yna gysylltiad canfyddedig rhwng CRhAau, ysgolion, a'r Cyngor. Mae'n bwysig felly bod safonau priodol o ran diogelu data a diogelwch taliadau yn cael eu cynnal.

Mae'r canllawiau hyn yn ymwneud â:

- Rheoliad Cyffredinol ar Ddiogelu Data y DU (GDPR y DU)
- Deddf Diogelu Data 1998
- Safon Diogelwch Data'r Diwydiant Cardiau Talu (SDD DCT)

2. Statws Cymdeithasau Rhieni ac Athrawon

Mae Cymdeithasau Rhieni ac Athrawon fel arfer yn:

- Elusennau annibynnol
- Endidau cyfreithiol ar wahân i'r ysgol
- Rheolwyr Data eu hunain o dan GDPR y DU

Fel Rheolwyr Data, mae CRhAau yn gyfrifol am benderfynu sut mae data personol yn cael ei brosesu ac am ddangos cydymffurfiaeth â deddfwriaeth diogelu data.

Ar ben hynny, lle mae CRhAau yn derbyn taliadau cerdyn debyd a chredyd, mae cydymffurfio â SDD DCT yn rhan o'u rhwymedigaethau cytundebol gyda'u darparwr talu a'r banc caffael, yn ogystal â rhoi sicrwydd i'r dinasyddion maen nhw'n eu gwasanaethu y bydd eu manylion ariannol yn aros yn ddiogel.

Mae canllawiau Swyddfa'r Comisiynydd Gwybodaeth yn ei gwneud yn glir bod yn rhaid i sefydliadau sy'n ymdrin â thaliadau cardiau debyd a chredyd weithredu mesurau diogelwch priodol yn unol â rhwymedigaethau diogelu data.

Ni all Cyngor Caerdydd gymeradwyo nac awdurdodi dyfeisiau, darparwyr neu lwyfannau talu penodol. Mae cyfrifoldeb am gydymffurfio yn gorwedd yn uniongyrchol gyda'r CRhA tra eu bod yn cymryd taliadau cerdyn debyd a chredyd.

3. SDD DCT – Gofynion Cydymffurfio Ymarferol

Pan fydd Cymdeithasau Rhieni ac Athrawon yn derbyn taliadau cerdyn debyd a chredyd (gan ddefnyddio dyfeisiau sglodyn a phin neu lwyfannau ar-lein), dylid ystyried y rheolaethau DCT canlynol.

3.1 Dyfeisiau Sglodyn a Phin

Dylai CRhAau sicrhau:

- Bod cyflenwr y ddyfais wedi'i ddilysu fel un sy'n cydymffurfio â DCT.
- Bod proses yn bodoli i gadarnhau bod y cyflenwr yn cynnal ei gydymffurfiaeth â DCT yn flynyddol.
- Bod tystiolaeth o gydymffurfiaeth y ddyfais wedi'i chael trwy wefan Cyngor Safonau Diogelwch y Diwydiant Cardiau Talu (CSD DCT).
- Bod Holiadur Hunanasesu wedi'i gwblhau lle mae'r CRhA yn defnyddio ei Rhif Adnabod Masnachwr (MID) ei hun.
- Bod unigolion sy'n defnyddio dyfeisiau wedi cael hyfforddiant sylfaenol ar:
    - Trin dyfeisiau yn ddiogel
    - Adnabod arwyddion o ymyrryd
- Bod gwiriadau rheolaidd yn cael eu cynnal i nodi achosion o ymyrryd, a bod y gwiriadau hyn yn cael eu cofnodi.
- Bod derbynebau'r masnachwr yn cael eu storio'n ddiogel a'u cadw yn unol â gofynion cadw Mastercard (sef am bum mlynedd ar hyn o bryd). Sylwer,
    - Mae'n hanfodol nad yw'r derbynebau'n arddangos Prif Rif y Cyfrif (PAN) yn llawn. Dim ond y chwe digid cyntaf a'r pedwar digid olaf ddylai fod yn weladwy.
    - Rhaid adolygu derbynebau bob chwarter, a phan fyddant wedi cyrraedd diwedd eu cyfnod cadw, rhaid cael gwared arnynt yn ddiogel (e.e. eu torri'n ddarnau mân iawn neu ddefnyddio gwasanaeth gwaredu gwastraff cyfrinachol).

3.2 E-Daliadau a Llwyfannau Talu Ar-lein

Pan gaiff taliadau cerdyn debyd a chredyd eu derbyn ar-lein neu o bell, dylai CRhAau sicrhau:

- Bod y darparwr talu yn cydymffurfio â DCT.
- Bod cydymffurfiaeth â DCT yn cael ei hadolygu a'i dilysu bob blwyddyn.
- Bod yna dystiolaeth ddogfennol o gydymffurfiaeth (e.e. cadarnhad bod Holiadur Hunanasesu neu Ardystiad Cydymffurfiaeth wedi'i gwblhau).
- Bod y CRhA yn cwblhau ei Holiadur Hunanasesu ei hun pan fydd yn gweithredu o dan ei Rhif Adnabod Masnachwr (MID) ei hun.

4. Cyfrifoldebau Diogelu Data (GDPR y DU)

Yn ogystal â rhwymedigaethau SDD DCT, rhaid i CRhAau gydymffurfio â GDPR y DU a Deddf Diogelu Data 2018.

Mae hyn yn cynnwys:

- Casglu data personol sy'n angenrheidiol at y diben a nodwyd yn unig.
- Sicrhau bod data personol yn cael ei brosesu'n gyfreithlon, yn deg ac yn dryloyw.
- Gweithredu mesurau diogelwch technegol a sefydliadol priodol.
- Cyfyngu mynediad i wirfoddolwyr awdurdodedig.
- Cadw gwybodaeth am gyhyd ag sydd angen yn unig.
- Darparu gwybodaeth breifatrwydd briodol i unigolion.
- Gall enghreifftiau o ddata personol sy'n cael ei brosesu gan CRhAau gynnwys:
- Manylion cyswllt rhieni a disgyblion
- Gwybodaeth am roddwyr
- Manylion gwirfoddolwyr
- Gwybodaeth cofrestru digwyddiadau

Gall methu â gweithredu mesurau diogelwch priodol olygu bod y CRhA yn agored i risg reoleiddiol a niwed i'w henw da. Fel y nodwyd uchod, yn aml mae yna gysylltiad canfyddedig rhwng CRhAau, ysgolion, a'r Cyngor ac felly gall hyn gyflwyno risgiau i'r sefydliadau hyn hefyd.

5. Rôl Ysgolion

Ysgolion sydd â'r wybodaeth a'r berthynas orau â Chymdeithasau Rhieni ac Athrawon, a gofynnir iddynt:

- Rhannu'r canllawiau hyn gyda'u CRhA neu gorff codi arian cyfatebol.
- Sicrhau bod CRhAau yn deall eu cyfrifoldebau fel Rheolwyr Data annibynnol.
- Cael sicrwydd bod CRhAau yn deall eu cyfrifoldebau wrth dderbyn taliadau cerdyn debyd a chredyd.
- Annog CRhAau i geisio cyngor annibynnol lle bo angen mewn perthynas â'u rhwymedigaethau cyfreithiol a chytundebol.

Natalie Blackler
Swyddog Cymorth Ysgolion - Llywodraethu Gwybodaeth
Ffôn: 07974842771
E-bost: DiogeluDataYsgolion@caerdydd.gov.uk